(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年5 月16 日 (16.05.2002)

PCT

(10) 国際公開番号
WO 02/39294 A1

(51) 国際特許分類[7]: G06F 15/00, H04Q 7/38, H04L 9/32

(21) 国際出願番号: PCT/JP01/09780

(22) 国際出願日: 2001 年11 月8 日 (08.11.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-344402
2000 年11 月10 日 (10.11.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社 エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11 番1号 Tokyo (JP).

(71) 出願人 (日本についてのみ): 株式会社 アニモ (ANIMO LIMITED) [JP/JP]; 〒231-0015 神奈川県横浜市中区尾上町二丁目27番 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 夏野 剛 (NATSUNO, Takeshi) [JP/JP]; 〒153-0062 東京都目黒区三田一丁目5-6 1002号 Tokyo (JP). 桑名隆滋 (KUWANA, Ryuji) [JP/JP]; 〒231-0015 神奈川県横浜市中区尾上町二丁目27番 株式会社 アニモ内 Kanagawa (JP).

(74) 代理人: 川崎研二(KAWASAKI, Kenji); 〒103-0027 東京都中央区日本橋一丁目2番10号 東洋ビルディング 7階 朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, BR, CA, CN, JP, KR, NO, NZ, PL, SG, US.

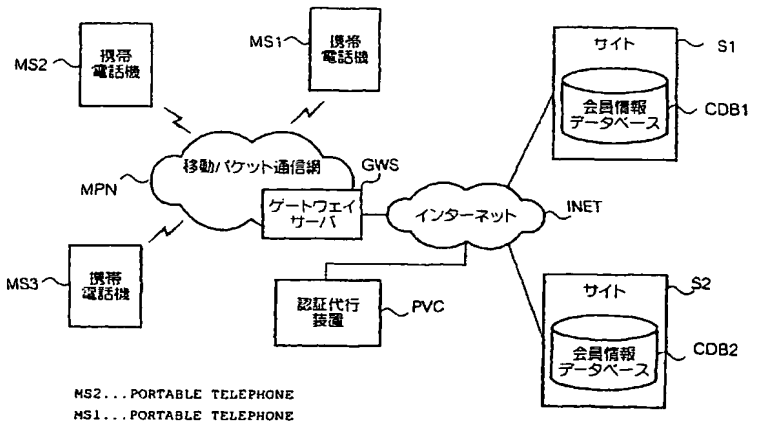
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: AUTHENTICATION SYSTEM, AUTHENTICATION AGENT APPARATUS, AND TERMINAL

(54) 発明の名称: 認証システム、認証代行装置および端末装置



(57) Abstract: An authentication system has a communication network, terminals, and an authentication agent apparatus. The authentication agent apparatus authenticates a user by using information including at least information fixed to a terminal or information unique to the user of a terminal, specifies a site that user desires, references the database containing authentication information needed when the user is to use the desired cite after authenticated, and agents for the authentication.

[続葉有]

WO 02/39294 A1

(57) 要約:

認証処理システムが、通信網と複数の端末装置と認証代行装置を有する。認証代行装置は、端末装置に固定された情報あるいは端末装置の使用者に固有の情報の少なくとも一つを含む情報を利用して使用者を認証し、使用者が希望するサイトを特定して、認証された使用者が希望するサイトを利用する時に必要となる認証情報を格納しているデータベースを参照して認証処理を代行する。

明 細 書

認証システム、認証代行装置および端末装置

技術分野

この発明は、通信網を介して会員にサービスを提供するサイトへ、会員の認証に必要な認証情報を渡すことで、端末装置を使用する会員による認証情報の手動入力を排除する認証システムと、この認証システムを構成する認証代行装置および端末装置に関する。

技術背景

インターネットの普及とともに、インターネットを介して、限定された会員にサービスを提供する会員制インターネット・サイトや利用者毎に内容の異なるサービスを提供するサイト（これらを、以降、会員制サイトあるいはサイトと称す。）が現われてきている。これらのサイトの運営者は、登録会員あるいは登録利用者（以降、会員と称す。）に対して固有のＩＤ（識別情報）とパスワード（このＩＤとパスワードをまとめて、これ以降、個別認証情報と称す。）を発行する。

ある会員が、あるサイトの提供するサービスを端末装置から利用しようとする時に、当該サイトは、当該会員の使用する端末装置に個別認証情報の入力フォームを送信して、個別認証情報の入力を要求する。当該会員は、この入力要求に対して、端末装置を操作して、個別認証情報を手動で入力する。当該サイトは、この個別認証情報を受信し、受信した個別認証情報が正しい場合に、この端末装置からのサービス利用要求が会員等からの利用要求であると認証する。認証された端末装置を使用する利用者は、以降、このサイトが提供する所望のサービスを利用することができる。

このような会員制サイトを複数利用する端末装置の使用者は、各々のサービスを利用するために、それぞれのサービスに対応した複数の個別認証情報を記憶する必要があった。複数のサービスに使用する個別認証情報を共通の

ものとすることができれば、利用者の記憶の問題は解決できるかもしれない。

しかし、実際には、個別認証情報の形式や属性は統一されてないから、サイト毎に異なっていることが多い。例えばあるサイトの個別認証情報は４～８文字からなる数字のみのＩＤと８～１２文字からなる英字のみのパスワードからなり、別のサイトの個別認証情報は９～１０文字の英数字からなるＩＤのみからなるということがある。また、サイトの個別認証情報を会員が自由に選択できない場合も多い。さらに、複数のサイトの個別認証情報を共通にすることはセキュリティの観点からも好ましくない。したがって、個別認証情報の共通化による個別認証情報の集約は困難であった。

たとえ個別認証情報の共通化ができた場合であっても、会員制サイトを利用する時に個別認証情報を手動で入力しなければならない点は不便なままであり、解決されていない。たとえば、端末装置の使用者が個別認証情報を入力して、ある会員制サイトのサービスを利用した後に、個別認証情報が共通している別の会員制サイトのサービスを利用するときに、個別認証情報をもう一度入力する必要があった。

個別認証情報の入力を省略する利用者にとって利便性の高い方法がある。

第１の例として、端末装置が個別認証情報の入力フォームを受信した時に、該当する入力フィールドに個別認証情報を自動入力させる方法がある。このようにすれば端末装置の使用者が個別認証情報を入力する手間を削減することができる。

しかし、この場合、個別認証情報が端末装置に記憶されていることになるから、この記憶されている個別認証情報が、第３者の手に渡って悪用されるおそれがある。また、セキュリティの観点からもこの方法は好ましくない。

第２の例として、グローバルＩＤサービスと呼ばれるサービスがある。

このサービスは、利用者に、利用する複数の会員制サイトの個別認証情報をこのサービスを提供するサイトに格納しておくこと手段を提供している。このサービスの利用者は、インターネットを介して当該サイトに、ＩＤとパスワードを入力してログインした後は、当該サイトが、当該利用者が利用しようとする会員制サイトからの要求を満たす個別認証情報を、個別の会員制

サイトに提供する。すなわち、このサービスの利用者は会員制サイト毎に個別認証情報を手動で入力する必要がなくなる。

しかし、グローバルサービスにログインするために必要なＩＤおよびパスワードが漏洩すると、当該サイトに格納されている全ての個別認証情報がまとまって漏洩することになる。すなわち、グローバルＩＤサービスを使うことにより、使用者が複数の個別認証情報を管理するよりも、個別認証情報の漏洩の危険性が増大することになるという問題があった。

発明の開示

本発明は、通信網と、前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、前記サイトに入力するに入力する個別認証情報を前記端末装置の使用者に対応して格納した第１のデータベースと、前記端末装置の使用者を当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する認証手段と、前記認証手段により認証された使用者が利用を希望するサイトを特定する特定手段と、第１のデータベースを参照して前記手段により認証された使用者と前記特定手段により特定されたサイトに対応した個別認証情報を抽出して、当該サイトに抽出された個別認証情報を渡す代行手段とを有し、前記通信網に接続した認証代行装置とを有する認証処理システムを提供する。

また、本発明の認証処理システムは、生体に固有な情報を使用して前記端末装置の使用者を認証することが好ましい。さらに、取得した生体に固有な情報の認証前段処理手段を有する前記端末装置を備えることがより好ましい。

また、本発明の認証処理システムは、前記使用者が認証レベルの選択を可能とする認証レベル選択手段を備えていることが好ましい。さらに、前記認証レベルに基づいて保険料を決定する保険料請求手段を供えていることがより好ましい。

また、本発明の認証処理システムは、認証の効果の有効期限を管理する認証有効期限管理手段を備えていることが好ましい。

また、本発明の認証システムは、前記第２のデータベースを、前記複数の

サイトが更新することを可能とする更新手段を備えていることが好ましい。

本発明の認証代行装置は、サイトに入力する個別認証情報を端末装置の使用者に対応して格納した第１のデータベースと、前記端末装置の使用者を当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する認証手段と、前記認証手段により認証された使用者が利用を希望するサイトを特定する特定手段と、第１のデータベースを参照して前記手段により認証された使用者と前記特定手段により特定されたサイトに対応した個別認証情報を抽出して、当該サイトに抽出された個別認証情報を渡す代行手段とを備える。

また、本発明の認証代行装置は、生体に固有な情報を使用して前記端末装置の使用者を認証することが好ましい。

本発明の端末装置は、通信網に接続することができる通信手段と、前記通信網を介してサイトおよび認証代行装置に接続することができる接続手段と、生体に固有な情報を取得する手段と、取得した生体に固有な情報を認証前段処理する手段を備える。

図面の簡単な説明

図１は、本発明の第１および第２の実施形態に係る認証システムの構成を示すブロック図である。

図２は、第１および第２の実施形態に係る認証代行装置ＰＶＣの構成を示すブロック図である。

図３は、認証用データベースＶＤＢ内の個人用テーブルＴ１の構成を例示する概念図である。

図４は、サイト情報データベースＳＤＢ内のサイト別テーブルＴ２の構成を例示する概念図である。

図５は、第１および第２の実施形態に係る形態に係る携帯電話機ＭＳの構成を示すブロック図である。

図６は、携帯電話機ＭＳが備える決定ボタン４１の概念図である。

図７は、携帯電話機ＭＳ２に表示される画面例を示す図である。

図８は、第１の実施形態に係る携帯電話機ＭＳ２の使用者が会員登録を行う場合の情報の流れを示す図である。

図９は、第１および第２の実施形態に係る携帯電話機ＭＳがＨＴＭＬデータ中に認証情報の入力タグが含まれた場合に行う処理の流れを示すフローチャートである。

図１０は、第１の実施形態に係る携帯電話機ＭＳ２の使用者がメニュー登録を行う場合の情報の流れを示す図である。

図１１は、第１の実施形態に係る認証代行装置ＰＶＣが行う認証代行処理の流れを示すフローチャートである。

図１２は、第１の実施形態に係る認証サービスを携帯電話機ＭＳ１の使用者が利用する場合の情報の流れを示す図である。

図１３は、携帯電話機ＭＳ１に表示される画面例を示す図である。

図１４は、第１の実施形態の認証サービスでおこなわれる認証処理を示す概念図である。

図１５は、第１の実施形態に係る認証サービスを携帯電話機ＭＳ１の使用者が複数のサイトＳ１、Ｓ２に利用する場合の情報の流れを示す図である。認証代行装置ＰＶＣが行う認証代行処理の流れを示すフローチャートである。

図１６は、携帯電話機ＭＳ３の使用者が認証代行サービスを受けようとした場合の情報の流れを示す図である。

図１７は、携帯電話機ＭＳ３に表示される画面例を示す図である。

図１８は、本実施形態に係る認証システムの認証レベルを示す図である。

図１９は第２の実施形態に係る認証サービスを携帯電話機ＭＳ１の使用者が利用する場合の情報の流れを示す図である。

発明を実施するための最良の形態

本発明をより詳細に説明するために、添付の図面に従ってこれを説明する。

＜Ａ．第１実施形態＞

＜Ａ－１．構成＞

＜Ａ－１－１．概要＞

図１は、本発明の第１の実施形態における認証システムの構成を示すブロック図である。同図に示すように、本実施形態における認証システムは、認証代行装置PVC、複数の携帯電話機ＭＳ（ＭＳ１～ＭＳ３）、複数の会員制サービス提供サイトＳ（Ｓ１～Ｓ２）、移動通信網MPN、インターネットINET、およびゲートウェイサーバGWSを有する。

本実施形態における認証システムに収容可能な携帯電話機ＭＳの数は任意であり、携帯電話機ＭＳの数は図示されている数に限定されない。本実施形態における認証システムに収容可能なサイトＳの数は任意であり、サイトＳの数は図示されている数に限定されない。

認証代行装置ＰＶＣは、インターネットに接続されている。認証代行装置ＰＶＣは、携帯電話機ＭＳの使用者が会員制サービス提供サイトＳ（Ｓ１～Ｓ２）の利用を開始する際に当該利用者がおこなう処理を代行する（認証代行処理と称す。）サービスを提供する。この認証サービスは会員制のサービスである。認証代行装置ＰＶＣは、当該サービスの会員に会員番号を与え、会員に全体認証情報を登録することを要求する。

携帯電話機ＭＳ（ＭＳ１～ＭＳ３）は、それぞれ移動通信網ＭＰＮに無線通信で接続することができる。

会員制サービス提供サイトＳ（Ｓ１～Ｓ２）は、インターネットに接続されている。サイトＳ（Ｓ１、Ｓ２）は、インターネットの利用者に対して会員制サービスを提供する。サイトＳ（Ｓ１、Ｓ２）は、サービスを利用する会員を認証するための個別認証情報を格納した会員情報データベースＣＤＢ（ＣＤＢ１、ＣＤＢ２）を有する。サイトＳは会員情報データベースに登録された会員にのみサービスを提供する。この個別認証情報は、会員番号（会員ＩＤ）および認証情報（パスワード）を含む。

本実施形態におけるサイトＳ１は、ＳＳＬ（Secure Sockets Layer）暗号化プロトコルを利用した通信(ＳＳＬ通信と称す)を利用できる会員にのみ、会員制サービスを提供している。

移動通信網ＭＰＮは、複数の基地局、複数の交換局、複数の関門中継交換局、複数の加入者処理装置、ゲートウェイサーバＧＷＳ、ならびにこれらを

接続する無線および有線通信回線を備えている。移動通信網ＭＰＮは、携帯電話機ＭＳ使用者に、携帯電話機ＭＳとインターネットＩＮＥＴとの間を中継する機能と当該移動通信網の利用料金を当該使用者に請求する機能を有する。

ゲートウェイサーバＧＷＳは、移動通信網ＭＰＮとインターネットＩＮＥＴを含む他のネットワークとを、ネットワーク間で異なる通信プロトコルの変換を行うことにより、相互接続する。ゲートウェイサーバＧＷＳは、移動通信網の関門中継交換局に備えることが好ましい。ゲートウェイサーバＧＷＳは、携帯電話機ＭＳからＨＴＴＰ（HyperText Transfer Protocol）プロトコルのＧＥＴ要求（以降、ＧＥＴ要求と称す）を受け取ると、当該ＧＥＴ要求に含まれるＵＲＩ（Uniform Resource Identifiers）を解析する。ゲートウェイサーバＧＷＳは、当該ＵＲＩが、インターネットＩＮＥＴ上を指し示す場合に、インターネットＩＮＥＴへ当該ＧＥＴ要求を転送する。ゲートウェイサーバＧＷＳは、インターネットＩＮＥＴから送信されてきた当該ＧＥＴ要求に対する応答を受信する。ゲートウェイサーバＧＷＳは、当該応答を携帯電話機ＭＳに送信する。

また、ゲートウェイサーバＧＷＳは、当該ＵＲＩが自己のリソースを示す場合には、当該ＧＥＴ要求に対応するリソースを、携帯電話機ＭＳに送信する。ゲートウェイサーバＧＷＳが保有するリソースは、ＨＴＭＬ（HyperText Markup Language）形式で記述された携帯電話機ＭＳのユーザインタフェースを定義するＵＩ定義情報を含む。

しかし、ゲートウェイサーバＧＷＳは、携帯電話機ＭＳがインターネットのあるサイトと、ＳＳＬ暗号化プロトコルを利用したＨＴＴＰ通信をしている時（https://で指定された場合）は、携帯電話機ＭＳと当該サイトの間の通信内容に関与しない。

＜Ａ－１－２．認証代行装置＞

図２は、本実施形態における認証代行装置ＰＶＣの構成を示すブロック図である。この図に示すように、本実施形態における認証代行装置ＰＶＣは、

認証用データベースＶＤＢ、サイト情報データベースＳＤＢ、通信部Ｐ１、操作部Ｐ２、表示部Ｐ３、記憶装置Ｐ４および制御部Ｐ５を有する。

認証用データベースＶＤＢは、さらに個人用テーブルＴ１を有する。図３は、個人用テーブルＴ１の構成を示す概念図である。同図に従って個人用テーブルＴ１について説明する。

個人用テーブルＴ１には、認証サービスの会員ごとにレコードが設けられている。各レコードは、固有の会員番号を記憶する会員番号フィールド、当該会員の呼称（名前）を記憶する名前フィールド、当該会員が使用する携帯電話機ＭＳの電話番号を記憶する電話番号フィールド、当該会員の認証（全体認証と称す）の基準となる情報（全体認証基準情報と称す）を暗号化して記憶する全体認証情報フィールド、認証レベルフィールド、全体認証の有効期限を記憶する有効期限フィールド、認証サービスの対象となる接続先のＩＤを記憶する接続先ＩＤフィールド、接続先に入力する個別認証情報を暗号化して記憶する個別認証情報フィールド、第３者による不正利用に対する保険料を記憶する保険料フィールド、認証サービスの使用料を記憶する使用料フィールドを有する。

さらに、個人用テーブルＴ１は、当該会員が利用する複数の接続先に対応して、複数の接続先ＩＤフィールドおよび当該接続先に対応した個別認証情報フィールドを有する。全体認証情報フィールドは、声紋情報フィールドと指紋情報フィールドにさらに分かれている。個別認証情報フィールドは、ＩＤフィールドとパスワードフィールドにさらに分かれる。

これらのフィールドのうち、会員番号、呼称（名前）、携帯電話機ＭＳの電話番号、当該会員の全体認証基準情報は、保険料、使用料の各フィールドには、会員登録時に、情報が格納される。

サイト情報データベースＳＤＢは、さらにサイト別テーブルＴ２を有す

図４は、サイト別テーブルＴ２の構成を示す概念図である。同図に従ってサイト別テーブルＴ２について説明する。

サイト別テーブルＴ２は、接続先ＩＤ毎にレコードを設ける。各レコードは、接続先ＩＤフィールド、接続先のタイトル名を格納するタイトルフィー

ルド、ＵＲＩを含む接続するため情報を記憶する接続情報フィールド、提供するサービスの分類フィールド、当該サービスを利用するためにＩＤの入力を要するか否かを示すＩＤ要否フィールド、当該サービスを利用するためにパスワードの入力を要するか否かを示すパスワード要否フィールド、ＩＤの入力を要する場合にはその属性（例えばバイト数）を記憶するＩＤ属性フィールド、パスワードの入力を要する場合にはその属性（例えばバイト数）を記憶するパスワード属性フィールドを有する。ここでＩＤ属性あるいはパスワード属性は、各会員制サービスが認証時に要求する個別認証情報に使用できる文字数、使用できる文字の種類を含む形式的要件である。さらに、図８３の個人用テーブルＴ１と図４のサイト別テーブルＴ２は、接続先ＩＤをキーとして関連付けられている。

通信部Ｐ１は、インターネットＩＮＥＴを介して他のノードと通信をすることができる。

操作部Ｐ２は、キーボード、ポインティングデバイスを備える。さらに操作指示やデータの入力のために使用する任意の装置を備えることができる。

表示部Ｐ３は、ディスプレイを備える。さらに任意の表示装置を備えることができる。

外部記憶装置Ｐ４は、電子ディスクやハードディスクを備える。さらに任意の外部記憶装置を備えることができる。

制御部Ｐ５は、ＣＰＵ（Central Processing Unit）５２と、インタフェースＰ５１と、ＲＯＭ(Read Only Memory)５３と、ＲＡＭ(Random Access Memory)５４とを有する。

インタフェースＰ５１は、ＣＰＵ５２と各部ＶＤＢ、ＳＤＢ、Ｐ１～Ｐ４を接続する。

ＣＰＵ５２は、インタフェースＰ５１を介して各部ＶＤＢ、ＳＤＢ、Ｐ１～Ｐ４を制御して、認証代行装置ＰＶＣに、起動処理＜Ａ－２＞、通信処理＜Ａ－３＞、会員登録処理（＜Ａ－４－３＞）、メニュー登録処理（＜Ａ－５－３＞）、認証代行処理（＜Ａ－６－３＞および＜Ａ－６－Ｂ＞）、保険・課金処理（＜Ａ－７＞）、サイト登録処理（＜Ａ－８＞）を含む処理を実行

させる。各処理については後述する。

ＲＯＭ５３は、ＣＰＵ５２が上記の各処理を実行するソフトウェア、ＣＰＵ５２が参照する各種データならびにその他のソフトウェアおよび情報を記憶する。

ＲＡＭ５４は、ＣＰＵ５２のワークメモリとして使用される。

本実施形態における認証代行装置ＰＶＣは、任意の数のＣＰＵを有することができる。本実施形態における認証代行装置ＰＶＣは、図２に示すように１ＣＰＵを有する装置で集中処理をしてもよいし、複数のＣＰＵを有する装置で分散処理をしてもよい。

＜Ａ－１－３．携帯電話機ＭＳ＞

図５は、本実施形態における携帯電話機ＭＳの１構成を示すブロック図である。同図に示すように、携帯電話機ＭＳは、通信部１、音響出力部２、音響入力部３、操作部４、表示部５および制御部６を有する。

通信部１は、無線通信を行うための、アンテナ、送信機および受信機を備える。通信部は移動通信網と無線通信をおこなうことができる。音響出力部２は、音源、スピーカおよび音を発するための装置を備える。

音響入力部３は、音声を入力するためのマイクを備える。

操作部４は、指示やデータの入力のためのキーパッド（図示しない）と、各種選択のためのボタン（図示しない）および決定ボタン４１を備える。

表示部５は、表示するための液晶ディスプレイを備える。

制御部６は、インタフェース６１と、ＣＰＵ６２と、ＲＯＭ６３と、フラッシュメモリ６４およびＲＡＭ６５を有する。

インタフェース６１は、ＣＰＵ６２と各部１～５を接続する。

ＣＰＵ６２は、インタフェース６１を介して各部１～５を制御して、携帯電話機ＭＳに、起動処理＜Ａ－２＞、通信処理＜Ａ－３＞、会員登録依頼処理（＜Ａ－４－２＞）、メニュー登録依頼処理（＜Ａ－５－２＞）、認証代行依頼処理（＜Ａ－６－２＞）を含む処理を実行させる。各処理については後述する。

ＲＯＭ６３は、ＣＰＵ６２が上記の各処理を実行するソフトウェア、ＣＰＵ６２が参照する各種データならびにその他のソフトウェアおよび情報を記憶する。特に、インターネット上のWWW（World Wide Web）サービスを携帯電話機ＭＳから利用できるようにするためのブラウザ（browser）ソフトウェア、および最初にブラウザがアクセスするＵＲＩ（ホームＵＲＩと称す。）として、ゲートウィイサーバＧＷＳ上のＵＩ情報が格納されているリソースを指定するＵＲＩが記憶されている。

本実施例におけるブラウザは、全体認証情報の入力タグを含むＨＴＭＬデータを取得すると、当該入力タグを識別することができる。さらに、当該ブラウザは、入力タグが指定する全体認証情報の入力を携帯電話機の使用者に促す画面を表示して、当該使用者により全体認証情報が入力されると、当該ＨＴＭＬデータの取得先に、入力された全体認証情報を送信することができる。本実施形態において全体認証情報の入力タグが指定する処理は、「音声信号の取得」と音声信号および指紋画像の取得」を含む。

フラッシュメモリ（不揮発性メモリ）６４は、ＣＰＵ６２から渡されたデータを記憶する

ＲＡＭ６５は、ＣＰＵ６２のワークメモリとして使用される。

（決定ボタン４１）

図６は、本実施形態における携帯電話ＭＳ１の操作部４に設けられる決定ボタン４１の内部構造を示す概略図である。

同図に示すように、決定ボタン４１の内部には、透過板４１１、透過板４１１を保持する支持部材４１２、携帯電話機筐体に固定して設けられた支持部材４１３、支持部材４１３に取り付けられたカメラ４２、光源４３、および透過板４１１、支持部材４１２、支持部材４１３、カメラ４２、光源４３で画定される内部空隙が設けられている。

透過板４１１および支持部材４１２は、図中上方から使用者の指によって押されると、図中下方に動き、押圧力が弱められると元の位置に戻るように構成されている。透過板４１１には、ガラスやアクリルを含む、透明素材あ

るいは半透明素材を使用することができる。

カメラ４２は、透過板４１１を介して透過板４１１を押圧する指の腹（指紋）を撮像するように配置されている。カメラ４２には、ＣＣＤ（Charge-Coupled Devices）カメラを使用することができる。

光源４３は、使用者の押圧する指が均等に照らし出されるように、カメラ４２の周囲に環状に配置されている。光源４３には、ＬＥＤ（Light Emitting Diode）を使用することができる。

＜Ａ－２．起動処理＞

認証代行装置ＰＶＣのＣＰＵ５２は、電源投入時に、ＲＯＭ５３に記憶されたソフトウェアを実行し、認証代行装置ＰＶＣに、ＳＳＬ通信、会員登録処理、メニュー登録処理、認証代行処理およびサイト登録処理の受付を開始させる。また、ＣＰＵ５２は、認証代行装置ＰＶＣに、保険・課金処理を開始させる。

携帯電話機ＭＳのＣＰＵ６２は、電源投入時に、ＲＯＭ５３に記憶されたソフトウェアを実行した後、操作部４から入力される指示を監視する。ＣＰＵ６２は、WWWサービスの利用開始を示す指示を検知すると、ＲＯＭ６３に記憶されたブラウザを実行する。ＣＰＵ６２は、無線通信部を制御して、携帯電話機ＭＳを移動通信網に接続させる。

ブラウザは、ゲートウェイサーバＧＷＳに、ＲＯＭ６２に記憶されているホームＵＲＩが指定するゲートウェイサーバ内に記憶されているＵＩ情報に対するＧＥＴ要求を送信する。

ＣＰＵ６２は、ＵＩ情報を受信すると、当該ＵＩ情報に基づいて、ユーザインタフェースを携帯電話機ＭＳの使用者に提供し、起動処理が完了する。この時、携帯電話機ＭＳの表示部５にはメインメニュー（例えば、図７の画面Ｇ１１１）が表示されている。

＜Ａ－３．通信処理＞

携帯電話機ＭＳで動作するブラウザが、ＳＳＬ通信要求を認証代行装置Ｐ

ＶＣに送信する。

認証代行装置ＰＶＣは、ＳＳＬ通信の開始要求を受信すると、ＳＳＬハンドシェークプロトコルにしたがって、当該携帯電話機ＭＳとハンドシェークを開始する。

認証代行装置ＰＶＣは、当該携帯電話機ＭＳとの間のセッションが新規に確立すると、ＳＳＬ通信を開始する。認証代行装置ＰＶＣは、当該セッションが確立されない場合は、ＳＳＬ通信を行わないで通信を終了する。このように、ＳＳＬ通信を利用することにより、送受信される情報（特に音声や指紋画像を含む情報）が第３者に悪用される危険性を小さくすることができる。

携帯電話機ＭＳは、サイトＳ１との間においてＳＳＬ通信をおこなう。

認証代行装置ＰＶＣは、サイトＳ１との間においてＳＳＬ通信をおこなうことができる。

＜Ａ－４．会員登録処理＞

＜Ａ－４－１．概要＞

図８は、本実施例における認証サービスを利用希望する者が、自己の所有する携帯電話機ＭＳ２から、本実施例における認証サービスに会員登録する場合の流れを示す図である。当該利用者および携帯電話機ＭＳ２の電話番号および携帯電話ＭＳ２の使用者の呼称（ここでは“Ｂ”）は、個人データベースＴ１に記憶されていないものとする。

（ステップ１０１）：携帯電話機ＭＳ２と認証代行装置ＰＶＣの間でＳＳＬ通信が開始する。

（ステップ１０２）：携帯電話機ＭＳ２は、ＳＳＬ通信が開始すると、認証代行装置ＰＶＣに、携帯電話機ＭＳ２の電話番号情報を含むＧＥＴ要求信号を送信する。

（ステップ１０３）：認証代行装置ＰＶＣは、ＧＥＴ要求信号を受信すると、携帯電話機ＭＳ２の使用者が、認証サービスの会員であるかどうかを判定する。

認証サービスの会員でないことを検知すると、携帯電話機ＭＳ２に、認証

レベル選択要求を含む信号を送信する。

認証サービスの会員であるときは、認証代行処理に進む。認証代行処理については後述する。

（ステップ１０４）：携帯電話機ＭＳ２は、認証レベル選択要求を含む信号を受信すると、使用者に認証レベルを選択する画面を表示する。

携帯電話機ＭＳ２は、使用者により認証レベルの選択が行われると、選択された認証レベル情報を、認証代行装置ＰＶＣに送信する。

（ステップ１０５）：認証代行装置ＰＶＣは、携帯電話機ＭＳ２に、基準情報入力フォームを含む信号を送信する。

（ステップ１０６）：携帯電話機ＭＳ２は、基準情報入力フォームを含む情報を受信すると、携帯電話機ＭＳ２の使用者に前提認証情報の入力を促す。

携帯電話機ＭＳ２は、使用者による全体認証情報が入力されると、入力された全体認証情報を、認証代行装置ＰＶＣに送信する。

（ステップ１０７）：認証代行装置ＰＶＣは、受信した全体認証情報の登録を終了し、会員登録を完了する。

本実施形態では、会員登録完了直後には全体認証を省略することができるので、認証代行装置ＰＶＣは、認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機ＭＳ２に送信する。パスポートメニュー信号については後述する。

＜Ａ－４－２．端末装置における会員登録依頼処理動作＞

（ステップ１０１）：携帯電話機ＭＳ２は、使用者により、メインメニュー（図７の画面Ｇ１１１）から「パスポート」が選択されると、認証代行装置ＰＶＣとの間でＳＳＬ通信を開始する。

（ステップ１０２）：携帯電話機ＭＳ２は、認証代行装置ＰＶＣに、携帯電話機ＭＳ２の電話番号を含むＧＥＴ要求を送信する。

（ステップ１０３）：携帯電話機ＭＳ２は、認証レベル選択要求を含む信号を受信すると、当該認証レベル選択要求に基づいて、認証レベルの選択を促す画面（例えば図７の画面Ｇ１３１）を表示部５に表示する。

（ステップ１０４）：携帯電話機ＭＳ２は、使用者によって、「音声のみ」が選択されると、「音声のみ」に対応した情報を含む認証レベル（本実施形態では「音声のみ」の場合に“１”と、「指紋情報および声紋情報」の場合に”３”とする。）を、認証代行装置ＰＶＣに送信する。

（ステップ１０５）：携帯電話機ＭＳ２は、基準情報入力フォームを受信すると、基準情報入力フォームに含まれる全体認証情報入力のタグを解釈する。先に選択した認証レベルが「音声のみ」を示す”１”であることから、携帯電話機ＭＳ２は、当該入力フォームに音声入力のタグを検知して、これを解釈し、音声の入力を促す画面（例えば図７の画面Ｇ１３２）を表示部５に表示する。（図９のステップＳＡ１、２）

（ステップ１０６）：携帯電話機ＭＳ２は、決定ボタン４１の使用者による押下げを検知すると、押下げ時点で音響入力部３から入力している音声を、全体認証情報として、認証代行装置ＰＶＣに送信し、会員登録以来処理を完了する。

＜Ａ－４－３．認証代行装置における会員登録処理動作＞

（ステップ１０１）：認証代行装置ＰＶＣと携帯電話機ＭＳ２の間でＳＳＬ通信が開始する。

（ステップ１０２）：認証代行装置ＰＶＣは、通信部Ｐ１を介して、非会員から送信されたＧＥＴ要求を受信する。

（ステップ１０３）：認証代行装置ＰＶＣは、受信したＧＥＴ要求に含まれる携帯電話ＭＳ２の電話番号をキーとして、個人用テーブルＴ１を検索する。

認証代行装置ＰＶＣは、当該電話番号を含むレコードが個人用テーブルＴ１に登録されていないことを検知すると、当該テーブルＴ１にレコードを追加する。

認証代行装置ＰＶＣは、当該追加したレコードの会員番号フィールドに、重複しない会員番号を生成して格納し、当該レコードの使用料フィールドに使用料“１００”を格納する。

認証代行装置ＰＶＣは、認証レベル選択要求を含む信号を、携帯電話機Ｍ

Ｓ２に送信する。

（ステップ１０４）：認証代行装置ＰＶＣは、受信した「音声のみ」を示す認証レベル”１”を、当該レコードの認証レベルフィールドに格納する。

（ステップ１０５）：認証代行装置ＰＶＣは、「音声のみ」を示す認証レベル”１”に対応して、全体認証情報として音声の入力タグおよび利用者の呼称の入力タグを含んだ基準情報入力フォームを含む信号を、携帯電話機ＭＳ２に送信する。

認証代行装置ＰＶＣは、当該認証レベル「音声のみ」を示す認証レベル”１”に応じた値“１００”（認証レベルが “２”の場合には“５０” 、“３”の場合には“０”）を当該レコードの保険料フィールドに格納する。

（ステップ１０６）：認証代行装置ＰＶＣは、全体認証情報として音声を受信する。

認証代行装置ＰＶＣは、受信した音声から声紋情報を生成して、この声紋情報を当該レコードの声紋情報フィールドに暗号化して格納する。

また、認証代行装置ＰＶＣは、使用者の呼称を含んだ情報を受信すると、受信した呼称を当該レコードの名前フィールドに登録する。

さらに、認証代行装置ＰＶＣは、現在時刻を取得して、現在時刻よりもある時間先となる時刻を有効期限として、当該レコードの有効期限フィールドに格納する。

有効期限の設定は、利用者がおこなえるようにできる。例えば、基準情報入力フォームに有効期限の入力タグを設けることによって実現できる。

また、個人テーブルＴ１にシフト時間フィールドを追加し、基準情報入力フォームにシフト時間の入力タグを設けることによって、有効期限をシフト時間という有効時間で決定することも可能である。

（ステップ１０７）：認証代行装置ＰＶＣは、（ステップ１０６）の処理が終了すると、会員登録処理を完了する。

認証代行装置ＰＶＣは、携帯電話機ＭＳ２にパスポートメニュー信号を含む信号を送信し、会員登録処理が完了する。本実施形態では、会員登録完了直後には全体認証を省略することができるので、認証代行装置ＰＶＣは、認

証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機ＭＳ２に送信する。

＜Ａ－５．メニュー登録処理＞

＜Ａ－５－１．概要＞

図１０は、本実施例における認証代行サービスの会員が、自己の所有する携帯電話機ＭＳ２から、認証代行装置ＰＶＣの提供する認証サービスにメニュー登録する場合の処理の流れを示す図である。携帯電話機ＭＳ２は全体認証が完了しているものとする。

ここで、携帯電話機ＭＳ２の電話番号および携帯電話機ＭＳ２の使用者の呼称（ここでは“Ｂ”）は、個人用テーブルＴ１に登録されているものとする。

（ステップ２０１）：携帯電話機ＭＳ２は、メニュー登録処理に移ることを示す選択情報を含む信号を、認証代行装置ＰＶＣに送信する。

（ステップ２０２）：認証代行装置ＰＶＣは、当該選択情報を含む信号を受信すると、複数のサイトの接続先ＩＤを含む登録選択メニューを含む信号を、携帯電話機ＭＳ２に送信する。

（ステップ２０３）：携帯電話機ＭＳ２は、当該登録選択メニューを含む信号を受信すると、サイトの選択を利用者に促す画面を表示する（例えば、図６の画面Ｇ１３４）。

携帯電話機ＭＳ２は、サイトが選択されると、選択されたサイトの接続先ＩＤを含む信号を、認証代行装置ＰＶＣに送信する。

（ステップ２０４）：認証代行装置ＰＶＣは、接続先ＩＤを含む信号を受信すると、個別登録フォームを含む信号を、携帯電話ＭＳ２に送信する。

（ステップ２０５）：携帯電話機ＭＳ２は、個別登録フォームを含む信号を受信すると、個別登録フォームに基づいて、当該サイトに対応した個別認証情報の入力を促す画面を表示する（例えば、図７のＧ１３５）。

携帯電話機ＭＳ２は、個別認証情報が入力されると、当該個別認証情報を含む信号を、認証代行装置ＰＶＣに送信する。

（ステップ２０６）：認証代行装置ＰＶＣは、個別認証情報を含む信号を受信すると、メニュー登録を行う。

認証代行装置ＰＶＣは、登録完了通知を含む信号を、携帯電話機ＭＳ２に送信する。

（ステップ２０７）：携帯電話機ＭＳ２は、登録完了通知を含む信号を受信すると、確認通知を含む信号を、認証代行装置ＰＶＣに送信する。

（ステップ２０８）：認証代行装置ＰＶＣは、確認通知を含む信号を受信すると、メニュー登録処理を完了する。本実施形態では、メニュー登録完了直後には全体認証を省略することができるので、認証代行装置ＰＶＣは、認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機ＭＳ２に送信する。

＜Ａ－５－２．携帯電話機ＭＳのメニュー登録依頼時の動作＞

（ステップ２０１）携帯電話機ＭＳ２は、パスポートメニュー信号から「新規登録」が利用者により選択されると、「新規登録」を選択したことを示す選択情報を含む信号を、認証代行装置ＰＶＣに送信する。

（ステップ２０２）携帯電話機ＭＳ２は、当該登録選択メニューを受信すると、認証代行の対象の登録を促す画面（例えば図７の画面Ｇ１３４）を表示部５に表示する。

（ステップ２０３）携帯電話機ＭＳ２は、使用者によって所望の対象（ここでは“懸賞クイズ”）が選択されると、この選択に対応した接続先ＩＤ（ここでは“５”）を、認証代行装置ＰＶＣに送信する。

（ステップ２０４）携帯電話機ＭＳ２は、個別認証登録フォームを受信すると、個別認証登録フォームに基づいて、ＩＤのみの入力を促す画面（例えば図７の画面Ｇ１３５）を、表示部５に表示する。

（ステップ２０５）携帯電話機ＭＳ２は、ＩＤ（ここでは“65883”）が使用者により入力され、送信ボタンの使用者による押下を検知すると、入力されたＩＤを、個別認証情報として認証代行装置ＰＶＣに送信する。

（ステップ２０６）携帯電話機ＭＳ２は、登録完了通知（あるいは書式違反

通知）を受信すると、接続先の新規登録が完了（あるいは失敗）した旨を使用者に通知する画面（例えば図７の画面Ｇ１３６あるいは画面Ｇ１３７）を表示部５に表示する。

（ステップ２０７）　携帯電話機ＭＳ２は、登録完了通知の画面あるいは書式違反通知の画面の“次へ”ボタンの使用者による押下げを検知すると、確認通知を認証代行装置ＰＶＣに送信し、メニュー登録依頼処理を成功（あるいは失敗）して終了する。

＜Ａ－５－３．認証代行装置ＰＶＣのメニュー登録処理時の動作＞

（ステップ２０２）認証代行装置ＰＶＣは、選択情報を含む信号を受信すると、認証代行の対象を選択するための登録選択メニューを、携帯電話機ＭＳ２に送信する。

この登録選択メニューは、選択可能な全ての接続先の接続先ＩＤおよびタイトルを含んでいる。（図１１のステップＳＢ１４）

（ステップ２０４）認証代行装置ＰＶＣは、接続先ＩＤを受信すると、当該接続先ＩＤで特定されるレコードを、サイト別テーブルＴ２から抽出する。

認証代行装置ＰＶＣは、当該レコードのＩＤ要否およびパスワード要否フィールドの内容（ここではＩＤを要するが、パスワードは不要）に対応した個別認証登録フォームを、携帯電話機ＭＳ２に送信する。（図１１のステップＳＢ１５）

（ステップ２０６）認証代行装置ＰＶＣは、ＩＤを受信すると、入力されたＩＤが、サイト別テーブルＴ２の当該レコードのＩＤ属性フィールドに記憶されたＩＤ属性（ここでは、４バイト以上８バイト以下であること）の条件に適合するか判定する。（図１１のステップＳＢ１６）

認証代行装置ＰＶＣは、当該ＩＤがＩＤ属性を適合すると、個人用テーブルＴ１の該当するレコード（会員番号が“２”のレコード）の接続先ＩＤおよびＩＤのフィールドに“５”および“65883”の組を追記する。

認証代行装置ＰＶＣは、登録完了通知を携帯電話機ＭＳ２に送信する。（図１１のステップＳＢ１７）

認証代行装置ＰＶＣは、当該ＩＤがＩＤ属性に適合しない場合、書式違反通知を、携帯電話機ＭＳ２に送信する（図１１のステップＳＢ１８）。

（ステップ２０８）：認証代行装置ＰＶＣは、確認通知を含む信号を受信すると、メニュー登録処理を完了する（図１１のステップＳＢ１９）。本実施形態では、メニュー登録完了直後には全体認証を省略することができるので、認証代行装置ＰＶＣは、認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機ＭＳ２に送信する。

＜Ａ－６．認証代行処理（パスポートメニュー）＞

＜Ａ－６－１．概要＞

図１２は、本実施例の認証サービスの会員が自己の所有する携帯電話機ＭＳ１から、認証代行装置ＰＶＣの提供する認証サービスを利用して、サイトＳ１が提供する会員制サービスを利用する場合の処理の流れを示す図である。

ここで、携帯電話機ＭＳ１の電話番号および携帯電話機ＭＳ１の使用者の呼称（ここでは“Ｃ”）は、個人用テーブルＴ１に登録されているものとする。

また、当該会員は、会員登録時に認証レベルに「音声＋指紋」を選択しているとする。

さらに、当該会員が携帯電話機ＭＳ１から最後に認証サービスを利用してから数時間以上経過しているものとする。

（ステップ３０１）認証代行装置ＰＶＣと携帯電話機ＭＳ１の間でＳＳＬ通信が開始する。

（ステップ３０２）携帯電話機ＭＳ１は、ＳＳＬ通信セッションが確立すると、認証代行装置ＰＶＣに、携帯電話機ＭＳ１の電話番号を含むＧＥＴ要求信号を送信する。

（ステップ３０３）認証代行装置ＰＶＣは、ＧＥＴ要求信号を受信すると認証情報入力フォーム情報を含む信号を、携帯電話機ＭＳ３に送信する。

（ステップ３０４）携帯電話機ＭＳ１は、認証情報入力フォーム情報を含む信号を受信すると、携帯電話機ＭＳ１の使用者に全体認証情報の入力を促す。

携帯電話機ＭＳ１は、使用者により全体認証情報が入力されると、入力された全体認証情報を、認証代行装置ＰＶＣに送信する。

（ステップ３０５）：認証代行装置ＰＶＣは、全体認証情報を受信すると、認証処理をおこなう。

認証代行装置ＰＶＣは、認証処理に成功すると、認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機ＭＳ１に送信する。

認証代行装置ＰＶＣは、認証処理に失敗すると、認証失敗通知を、携帯電話機ＭＳ１に送信し、認証代行処理を失敗して完了する。

（ステップ３０６）携帯電話機ＭＳ１は、パスポートメニュー信号から、一つのサイトが使用者によって選択されたことを検出すると、当該サイトの情報を含む選択情報を、認証代行装置ＰＶＣに送信する。

（ステップ３０７）認証代行装置ＰＶＣは、選択情報を受信すると、個別ログイン情報を生成して、当該個別ログイン情報を、携帯電話機ＭＳ１に送信する。

（ステップ３０８）携帯電話機ＭＳ１は、個別ログイン情報を受信すると、当該個別ログイン情報に記載されている方法で、サイトＳ１との間でＳＳＬ通信を開始する。

（ステップ３０９）：携帯電話機ＭＳ１は、ＳＳＬ通信が開始すると、当該個別ログイン情報に記載されている方法で、サイトＳ１にログインする。

サイトＳ１は、携帯電話機ＭＳ１の使用者のログインについて、会員情報データベースＣＤＢ１を参照して認証処理を行う。

（ステップ３１０）サイトＳ１は、当該使用者の認証に成功すると、利用者にコンテンツの提供を含む会員制サービスの提供をおこなう。

サイトＳ１は、当該使用者の認証に失敗すると、認証処理を終了する。

＜Ａ－６－２．携帯電話ＭＳにおける認証代行依頼処理の動作＞

（ステップ３０１）携帯電話機ＭＳ１は、メインメニュー（図７の画面Ｇ１１１）から「パスポート」を携帯電話機ＭＳ１の使用者により選択されたことを検知すると、認証代行装置ＰＶＣとの間でＳＳＬ通信を開始する。

（ステップ３０２）：携帯電話機ＭＳ１は、認証代行装置ＰＶＣに、携帯電話機ＭＳ１の電話番号を含むＧＥＴ要求を送信する。

（ステップ３０３）携帯電話機ＭＳ１のＣＰＵ６２は、「音声信号および指紋画像の取得」を指定するタグを含む全体認証情報入力フォームを受信すると、当該入力タグに基づいて、全体認証情報の入力を促す画面（例えば図１５の画面Ｇ１１２）を表示部５に表示する。

（ステップ３０４）ＣＰＵ６２は、決定ボタン４１の使用者による押下げを検知すると、ＬＥＤ光源４３を点灯して、ＣＣＤカメラ４２に写る像を記録（撮像）する。

この時、ＣＣＤカメラ４２は、決定ボタン４１を押し下げている指の腹を、透過板４１１越しに撮像する。

ＣＰＵ６２は、決定ボタン４１の使用者による押下げ時に、音響入力部３から入力していた音声を取得する。（図９のステップＳＡ１、３）

ＣＰＵ６２は、撮像された指紋画像と音声を、全体認証情報として認証代行装置ＰＶＣに送信する。

（ステップ３０５）携帯電話機ＭＳ１は、パスポートメニュー信号を受信すると、認証代行の対象の選択を促す画面（例えば図１３の画面Ｇ１５１）を、表示部に表示する。

（ステップ３０６）携帯電話機ＭＳ１は、サイト「Ｄ社ポイント」が使用者によって選択されたことを検知すると、このサイトを選択したことを示す選択情報を、認証代行装置ＰＶＣに送信する。

（ステップ３０８） 携帯電話機ＭＳ１は、個別ログイン情報を受信すると、当該個別ログイン情報に記述されているサイトＳ１とＳＳＬ通信を開始する。

（ステップ３０９）携帯電話機ＭＳ１は、サイトＳ１とＳＳＬ通信が開始するのを待って、当該個別ログイン情報に記述されているＧＥＴ要求のシーケンスを、個別ログイン情報に記述されているサイトＳ１で個別認証処理をおこなっているリソース“//www.c.co.jp/point/point.cgi”に送信する。この送信によって、手動でのログイン手続きの代行をおこなっている。

（ステップ３１０）サイトＳ１は、当該ＧＥＴ要求を受信すると、携帯電話

機ＭＳ１の認証処理を開始する。ＩＤとパスワードに“docom”と“********”がそれぞれ正しく入力されているので、携帯電話機ＭＳ１の使用者はサイトＳ１の提供するサービスの会員であると認証される。

サイトＳ１は、以降、当該使用者の個人用サービスコンテンツ（情報）を携帯電話機ＭＳ１に送信する。（ここでは当該サイトＳ１が提供するショッピングサービスの利用で取得した当該携帯電話機ＭＳ１の累計ポイントを示す情報が送信されている。）

携帯電話機ＭＳ１は、当該コンテンツを受信すると、使用者が取得したポイントを通知する画面（例えば図７の画面Ｇ１５２）を、表示部５に表示する。

＜Ａ－６－３．認証代行装置ＰＶＣの認証代行処理時の動作＞

（ステップ３０１）認証代行装置ＰＶＣと携帯電話機ＭＳ１はＳＳＬ通信を開始する。（図１１のステップＳＢ１）

（ステップ３０２）認証代行装置ＰＶＣは、携帯電話機の電話番号を含むＧＥＴ要求信号を受信すると、個人用テーブルＴ１参照して、当該電話番号を含むレコードを検索する。認証代行装置ＰＶＣは、検索に成功すると、当該レコードを抽出する。ここでは、会員番号フィールドに“１”が格納されたレコードが抽出される。（図１１のステップＳＢ２）

認証代行装置ＰＶＣは、現在時刻を取得して、当該レコードの有効期限フィールドと時刻の比較をおこなう。ここでは、最後に認証サービスを受けてから長時間経過しているので、全体認証は有効期限切れである。（図１１のステップＳＢ４）

（ステップ３０３）認証代行装置ＰＶＣは、当該レコードの認証レベルが”２”であるから、「音声信号および指紋画像の取得」を指定する入力タグを含む認証情報入力フォームを、携帯電話機ＭＳ１に送信する。（図１１のステップＳＢ５）。

（ステップ３０４）　認証代行装置ＰＶＣは、全体認証情報として音声および指紋画像を受信する。（図１１のステップＳＢ５）

認証代行装置ＰＶＣは、これらの音声および指紋画像から声紋情報および指紋情報を生成する。

認証代行装置ＰＶＣは、当該声紋情報および指紋情報と、先に選択したレコードに格納されている全体認証基準情報（ここでは声紋基準情報および指紋基準情報）と照合する。

この時、認証代行装置ＰＶＣは、当該レコードに暗号化されて記憶されていた全体認証基準情報を読み出す時に暗号解読して、照合に使用して、照合完了後に破棄する。このようにして、基準情報の漏洩を防止している。（図１１のステップＳＢ６）

図１４は、認証代行装置における認証処理過程の流れを示す図である。同図に示すように、認証処理過程は、フィルタ処理、周波数分析処理、特徴抽出処理、特徴正規化処理、照合を含む。

（フィルタ処理）：認証代行装置ＰＶＣは、受信した生体固有情報（ここでは、指紋画像あるいは音声）を含んだ生データから有用な情報を含む帯域以外の信号を除去する。

（周波数分析処理）：認証代行装置ＰＶＣは、フィルタにかけられたデータについて、空間あるいは時間周波数分析処理を行う。

（特徴抽出処理）：認証代行装置ＰＶＣは、周波数分析処理された信号から対象となる生体情報を特徴付ける特徴パラメータを抽出する。

（特徴正規化処理）：認証代行装置ＰＶＣは、得られた個々の特徴パラメータを正規化して、正規化特徴パラメータを得る。

（照合）：認証代行装置ＰＶＣは、前記正規化特徴パラメータと全体認証基準情報を照合する。本実施形態における照合の方法は、パターンマッチング法を含む方法を採用することができる。

認証代行装置ＰＶＣは、照合に成功すると、現在時刻からある時間（例えば３０分)経過させた時刻を当該レコードの有効期限フィールドに格納する。（図１１のステップＳＢ８）

（ステップ３０５）認証代行装置ＰＶＣは、個人テーブルＴ１を参照して、認証に成功した携帯電話機の使用者のレコードを参照して、当該使用者が、

登録してある複数の接続先ＩＤを抽出し、抽出した接続先ＩＤをキーとして、サイトテーブルＴ２を参照して、接続先ＩＤに対応したレコードから、サイトのタイトルおよび分類を抽出する。

認証代行装置ＰＶＣは、抽出した接続先のタイトル名と接続先ＩＤ情報を含むパスポートメニュー信号を生成する。ここでは、接続先ＩＤが“７”の接続先に対応したタイトル「Ｄ社ポイント」および接続先ＩＤ”７”ならびに、接続先ＩＤが“５”の接続先に対応したタイトル「懸賞リスト」および接続先ＩＤ”５”を含むパスポートメニュー信号を生成する。

本実施例では、さらに、パスポートメニュー信号に、「新規登録」というタイトルの接続情報が認証代行装置ＰＶＣによって付け加えられている。

認証代行装置ＰＶＣは、このように生成された認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機ＭＳ１に送信する（図１１のステップＳＢ９）。

（ステップ３０６）認証代行装置ＰＶＣは、選択情報を受信すると、当該選択情報の種別を判定する。認証代行装置ＰＶＣは、当該選択情報が新規メニュー登録を要求する場合には、メニュー登録処理に移行する（図１０ステップＳＢ１２）。ここでは、接続先ＩＤ“７”が選ばれたとする。

（ステップ３０７）認証代行装置ＰＶＣは、当該選択情報に含まれる接続先ＩＤをキーとして、テーブルＴ１およびＴ２を参照して、個別ログイン情報を生成する。

この個別ログイン情報は、その解釈・実行時にＧＥＴ要求を自動的に送出するように記述されたＨＴＭＬデータであり、当該接続先ＩＤに対応した接続先のへ個別認証情報を渡す旨のシーケンスが当該ＧＥＴ要求に含まれるように記述されている。ここでは、接続先ＩＤ“７”、タイトル「Ｄ社ポイント」であるサイトが要求する個別ログイン情報と会員番号“１”から、個別ログイン情報が生成される。

認証代行装置ＰＶＣは、当該個別ログイン情報を携帯電話機ＭＳ１に送信し、認証代行処理を完了する（図１１のステップＳＢ１３）。

＜Ａ－６Ｂ．全体認証情報入力の有効期限と全体認証入力省略場面＞

図１０に示す認証代行装置のフローチャートには、全体認証入力が省略されて個別認証代行処理が行われる２つのケースが示されている。

第１のケースでは、認証代行装置ＰＶＣは、会員登録（ステップＳＢ３）を完了すると、（ステップＳＢ２）から（ステップＳＢ４）の処理に進む。このケースでは、有効期限が、会員登録時に会員登録時点より経過した時刻として設定されたばかりであるから、その時点は全体認証の有効期限内にあると判定される。したがって、認証代行装置ＰＶＣは、全体認証処理を省略して、パスポートメニュー（ステップＳＢ９）に進むことができる。このように、会員登録後に利用者にパスポートメニューを使用することを許可している。この間、携帯電話の画面は、例えば、図７の画面Ｇ１３２－Ｇ１３８－Ｇ１３９のように変化する。

第２のケースでは、認証代行装置ＰＶＣは、メニュー登録が完了する（ステップＳＢ１９）と、（ステップＳＢ４）に進む。この時点で、全体認証が有効期限内となるように、有効期限を設定しておくことによって、利用者は、メニュー登録でパスポートメニューに新規に追加したサイトを選んで認証サービスを受けることができる。ただし、サイト登録中に全体認証情報入力の有効期間を経過した場合には、全体認証情報入力を再度しなければならない。

第３のケースは、図１５に示す本実施形態における認証サービスの会員が、自己の所有する携帯電話機ＭＳ１を使用して、サイトＳ１を利用した後に、サイトＳ２を利用する場合である。この間、携帯電話の画面は、例えば、図１３の画面Ｇ１５１－Ｇ１５２－Ｇ１５１－Ｇ１５３のように変化する。ただし、サイトＳ１利用中に全体認証情報入力の有効期間を経過した場合には、サイトＳ２を利用する時に、全体認証情報入力を再度しなければならない。

このようにして、認証代行装置ＰＶＣは、全体認証情報入力の有効期限を管理することによって、利用者の利便性とセキュリティのバランスを保っている。

＜Ｃ－６Ｃ．認証サービスの不正利用時＞

ここでは、認証代行サービスの正当な会員（会員番号は“３”）が所有する携帯電話機ＭＳ３を拾った第３者（以後、使用者）が認証代行サービスを受けようとした場合を想定している。なお、使用者が携帯電話機ＭＳ３を拾ったのは、正当な会員が最後に認証代行サービスを利用してから数時間経過した時点とする。

この場合、図１６に示すように、使用者が携帯電話機ＭＳ３を操作し、メインメニュー（図１７の画面Ｇ１１１）から「パスポート」を選択すると、携帯電話機ＭＳ３から認証代行装置ＰＶＣへ接続要求が送信され、両者の間でＳＳＬのハンドシェークが行われ、両者間でＳＳＬ通信が可能となる（図１１のステップＳＢ１）。

次に、携帯電話機ＭＳ３から認証代行装置ＰＶＣへ、「パスポート」の選択に応じたＧＥＴ要求が送信される。このＧＥＴ要求を受信した認証代行装置ＰＶＣでは、当該ＧＥＴ要求に含まれている電話番号をキーとして個人用テーブルＴ１が検索され（図１１のステップＳＢ２）、結果として、会員番号フィールドに“３”が格納されたレコードが抽出される。このレコードの有効期限フィールドには現在時刻以前の時刻が格納されていることから、このレコードに基づいた認証情報入力フォームが、ＧＥＴ要求の応答として認証代行装置ＰＶＣから携帯電話機ＭＳ３へ送信される（図１１のステップＳＢ４，ＳＢ５）。なお、会員番号フィールドに“３”が格納されたレコードの認証レベルフィールドには“１”が格納されていることから、認証情報入力フォーム中の入力タグは、「音声信号の取得」を指定するタグとなる。

この認証情報入力フォームを受信した携帯電話機ＭＳ３では、当該認証情報入力フォームが解釈・実行され、全体認証情報の入力を促す画面（例えば図　　の画面Ｇ１１２）が表示される。この画面を視認した使用者が発音しながら決定ボタン４１を押すと、その時点で音響入力部３から入力されている音声信号が、全体認証情報として認証代行装置ＰＶＣへ送信される。

全体認証情報として音声信号を受信した認証代行装置ＰＶＣでは、この音声信号から声紋情報が生成され、この声紋情報と、先に選択したレコードに格納されている声紋情報とが照合される(図１１のステップＳＢ５，ＳＢ６)。

後者の声紋情報は正当な会員の声紋情報であることから、両者が一致することはない。よって、認証代行装置ＰＶＣでは認証に失敗したと判断され、携帯電話機ＭＳ３から認証代行装置ＰＶＣへ認証失敗通知が送信される（図１１のステップＳＢ７，ＳＢ１０）。この結果、携帯電話機ＭＳ３には、全体認証に失敗した旨を示す画面(例えば図１７の画面Ｇ１１２)が表示される。

＜Ａ－７．保険、課金処理＞

本実施例の認証システムは、利用者が会員登録時に、選択した全体認証に利用する認証レベルに基づいて保険料が定められる。本実施例では、認証レベルとして１から３が提供され、図１８に示すように、それぞれ利用する照合情報と保険料が設定されている。

認証代行装置ＰＶＣは、利用者が選択した認証レベルを個人データベースＴ１の認証レベルフィールドに格納し、保険料フィールドに当該認証レベルに対応する保険料を格納する。

認証代行装置ＰＶＣは、ある時点で、個人用テーブルＴ１の当該フィールドに格納されている保険料と使用料を合計した金額を、端末装置の複数の使用者に、それぞれ請求する。

認証代行装置ＰＶＣは、この時、上記金額と端末装置の電話番号を含む請求情報を生成して、これを移動通信網ＭＰＮへ送信することによって、移動通信網ＭＰＮに課金処理を依頼しても良い。

移動通信網ＭＰＮは、この請求に通信料を加えた金額を、端末装置の使用者に請求する。

＜Ａ－８．サイト登録処理＞

本実施形態の認証システムは、認証代行装置ＰＶＣのサイト別テーブルＴ２にレコードを追加する機能を有する。

認証システム代行装置ＰＶＣは、エージェントプログラムを実行することによって、インターネットに接続された会員制サービスを提供しているサイトの情報を収集し、当該サイトそれぞれについて、自動的にサイト別テーブ

ルＴ２にレコードを追加して、サイト登録を行うようにしてもよい。

このエージェントプログラムは、会員がＩＤやパスワードをサイト毎に記述された認証プログラムに渡す旨のシーケンスが記述されたＨＴＭＬデータを、インターネット上で収集する。このエージェントプログラムは、収集したＨＴＭＬデータを解析して、当該ＨＴＭＬデータに記述されているＩＤ入力やパスワード入力を示すタグを検出して、当該ＩＤやパスワードに要求される属性（使用できる文字数、使用できる文字種を含む情報）を判別して、サイト別データベースＴ２のＩＤ属性およびパスワード属性フィールドに格納する。

さらに、このエージェントプログラムは、収集したＨＴＭＬデータを得たサイトに含まれるタグで指定された情報に基づいて、当該サイトの分類を試み、サイト別データベースＴ２の当該サイトに対応するレコードの分類フィールドに、得られた分類名を格納するようにしてもよい。

また、本実施形態の認証代行装置ＰＶＣは、外部（例えばサイトＳ１の運営者）の指示に従い、サイト別テーブルＴ２の任意のレコード内の接続情報、分類、ＩＤ要否、パスワード要否、ＩＤ属性、およびパスワード属性のフィールドの内容を変更する機能を有する。

＜Ｂ．第２実施形態＞

本発明の第２の実施形態における認証システムの構成は、図１のブロック図に示す第１の実施形態と同一構成をとる。

＜Ｂ－１．認証代行処理＞

図１９は、本実施例における認証サービスをの会員が、自己の所有する携帯電話機ＭＳ３から、認証代行装置ＰＶＣの提供する認証サービスを利用して、サイトＳ１が提供する会員制サービスを利用する場合の処理の流れを示す図である。

ここで、認証サービスを利用する携帯電話機ＭＳ３の使用者は、会員登録時に、認証レベル”１”「声紋情報を使用する」ことを選択してあるとする。

また、認証代行サービスの利用者は、充分長い時間、認証代行サービスを

利用していなかったとする。

図１９に示される処理と、図１２に示される第１の実施例における認証処理は共通部分が多いので、異なる部分についてのみ説明を加える。

（ステップ４０３）携帯電話機ＭＳ３のＣＰＵ６２は、「音声信号の取得」を指定するタグを含む全体認証情報入力フォームを受信すると、当該入力タグに基づいて、全体認証情報の入力を促す画面（例えば図１３の画面Ｇ１１２）を表示部５に表示する。

（ステップ４０４）ＣＰＵ６２は、決定ボタン４１の使用者による押下げ時に、音響入力部３から入力していた音声を取得する。

ＣＰＵ６２は、取得した音声について、認証処理前段処理を行う。

本実施例において認証処理前段処理はフィルタ処理、周波数処理、特徴抽出処理および特徴正規化処理を含む。

携帯電話機ＭＳ１は、当該前段処理が行われると、正規化特徴情報を、認証代行装置ＰＶＣに送信する。

（ステップ４０５）認証代行装置ＰＶＣは、正規化特徴情報を受信すると、認証処理後段処理として、受信した正規化特徴情報と、個人テーブルＴ１の該当するテーブルに記憶されている全体認証基準情報とを照合する。

認証代行装置ＰＶＣは、照合に成功すると、携帯電話機ＭＳ３に、パスポートメニュー信号を送信する。

＜Ｃ．変形例＞

＜Ｃ－１．変形例１＞　本実施形態の認証システムは、携帯電話機ＭＳに固定されている電話番号をキーとして個人用テーブルＴ１を検索して、全体認証処理をしているが、電話番号の代わりに携帯電話機ＭＳの使用者のＩＤをキーとして個人用テーブルＴ１を検索して、全体認証処理をしてもよい。さらに電話機使用者の生体情報をキーとして個人用テーブルＴ１を検索して、全体認証処理をしてもよい。この場合、本実施例の認証サービスの利用者は、他人の携帯電話機ＭＳを借用して、当該サービスを利用することができるようになる。

＜Ｃ－２．変形例２＞　本実施形態の認証システムは、声紋情報の照合を全体認証において必ず実行しているが、認証システムは声紋情報の照合を実行しないで、指紋情報の照合を実行するようにしてもよい。この場合、認証代行装置は個人用テーブル１の該当する使用者のレコードの認証レベルフィールドに、例えば、認証レベル“２”を書き込む。また、認証代行装置ＰＶＣは当該レコードの保険料フィールドに、保険料“５０”を書き込む。

＜Ｃ－３．変形例３＞　本実施例の認証システムは、虹彩パターン、　　、を含む生体固有情報を含む全体認証情報を利用してもよい。さらに、本実施例の認証システムは、生体情報でない高いセキュリティを確保できる情報を含む全体認証情報を利用してもよい。

＜Ｃ－４．変形例４＞　本実施形態の認証システムは、携帯端末の契約者以外が使用することが可能なようにしても良い。例えば契約者本人が怪我をして、全体認証情報を入力できなくなった場合に、代理人が認証代行サービスを利用できるように、個人用テーブルＴ１の当該契約者のレコードに代理人用フィールドを追加して、当該フィールドに代理人の声紋情報（および指紋情報）を格納してもよい。この時、代理人が声紋情報（および指紋情報）を格納する方法は任意である。

＜Ｃ－５．変形例５＞　本実施形態の認証代行装置ＰＶＣは、ゲートウェイサーバＧＷＳを兼ねていてもよい。この場合は、認証代行装置ＰＶＣは、ゲートウェイサーバＧＷＳが認証する携帯電話機ＭＳの発（コーラー）ＩＤを端末装置に固定された情報として利用して全体認証処理をおこなうことができる。さらにこの場合、セキュリティを確保できるならば、移動通信網ＭＰＮ内にある携帯電話機と認証代行装置ＰＶＣ（＝ゲートウェイサーバＧＷＳ）間では非暗号化通信をおこない、ゲートウェイサーバＧＷＳとサイトＳ（Ｓ１－Ｓ２）間でのみ暗号化通信をおこなうようにしてもよい。すなわち、サ

ーバとサーバとの間でのみ暗号化通信を行うようにしてもよい。

＜Ｃ－６．変形例６＞　本実施例の認証システムは、利用者がパスポートメニュー信号に登録されていないサイトを認証サービスの対象（すなわちパスポートメニュー信号）に追加登録することができるようにしてもよい。

携帯電話ＭＳの利用者は、メニュー登録時に、パスポートメニュー信号に登録されていないサイトを追加する旨を指定して、追加希望サイトのタイトル、接続情報、分類、ＩＤおよびパスワードの要否、個人認証情報（ＩＤ、パスワード）を手動で入力する。

認証代行装置ＰＶＣは、追加希望サイトの情報を受信すると、個人テーブルＴ１の当該利用者のレコードに当該追加サイトの情報を格納する。この時、認証代行装置ＰＶＣは、サイト別テーブルＴ２を参照して、重複しない接続先ＩＤを付与する。

認証代行装置ＰＶＣは、個人テーブルＴ１にサイトの接続情報を格納する新たなフィールドを追加することによって、当該サイトの追加をおこなっても良い。

あるいは、認証代行装置ＰＶＣは、サイト別テーブルＴ２にレコードを追加して、受信した追加サイトの情報を当該レコードに格納することによって、当該サイトの追加をおこなっても良い。さらに、認証代行装置ＰＶＣは、利用者にＩＤおよびパスワードの要否の入力を求めないで、受信した個人認証情報を解析してＩＤおよびパスワードの要否を判定するようにしても良い

＜Ｃ－７．変形例７＞　本実施形態の端末装置は、ブラウザを搭載した携帯電話機に限定されない。本実施形態の端末装置は：固定電話機に接続して使用される、据え置き型コンピュータやブラウザを搭載したセットトップボックスを含むクッキー（Cookie）を取り扱うことができるクッキー対応端末装置；固定電話機に接続して使用される、ＰＤＡ（Personal Data Assistant）や携帯ゲーム機器を含むクッキーを取り扱うことができないクッキー非対応端末装置；ＳＩＭ（Subscriber Identity Module）やＵＩＭ（User Identity

Module）と組み合わせて使用する携帯電話機能を有するクッキー対応端末装置；携帯電話機に接続して使用されるクッキー対応端末装置；携帯電話機に接続して使用されるクッキー非対応端末装置；ＳＩＭやＵＩＭと組み合わせて使用するクッキー非対応端末装置を含む。

本実施例におけるクッキーを使用することができる端末装置は、使用者を特定するＩＤをクッキーに記録して、このＩＤを端末装置に固定された情報として、全体認証処理で利用しても良い。

また、本実施例における携帯電話機（あるいはＳＩＭやＵＩＭ）を使用する端末装置は、携帯電話機（あるいはＳＩＭやＵＩＭ）に固定された電話番号を、端末装置に固定された情報として、全体認証処理で利用しても良い。

さらに、本実施例における携帯電話機は、クッキーを使用することができる携帯電話機も含む。この時、本実施例におけるクッキーを使用することができる携帯電話機は、使用者を特定するＩＤをクッキーに記録して、このＩＤを携帯電話機に固定された情報として、全体認証処理で利用しても良い。

＜Ｃ－８．変形例８＞

本実施形態の端末装置は、指紋画像を入力する機能を備えていない携帯電話機ＭＳを含むものとする。さらに、本実施形態の端末装置は、全体認証情報入力タグを判別することができない携帯電話機ＭＳも含む。

本発明は上述した具体的な態様に限定されるのもではなく、特許請求の範囲に記載された範囲内で任意の態様を含む。

＜Ｄ．補足＞

このように、本実施形態によれば、携帯電話機の使用者は、ＩＤやパスワードの入力を要する、セキュリティの確保された各種の個人用サービスを利用する際に、個別の認証情報（ＩＤやパスワード）を記憶しておく必要がない。さらに、個別認証情報は携帯電話機に記憶されないため、携帯電話機が第３者の手に渡っても、個別認証情報が漏洩する虞はない。

また、本実施形態によれば、第３者が認証代行サービスを不当に利用する

事態を確実に回避することができる。特に、全体認証情報として声紋情報や指紋情報等の生体情報を利用するようにしたことにより、パスワードや暗証番号を用いる場合に比較して、本人性の認証をより確実に行うことができる。さらに、生体情報は使用者による記憶を要さないため、使用者にかかる負担が軽減されるという利点もある。

さらに、本実施形態によれば、指紋画像の取得機能を持たない携帯電話機ＭＳ２を用いる使用者に対しても認証サービスを提供することができる。したがって、使用者は使用中の端末を買い換えることなくサービスを受けることができる。また、音声を入力する機能を備えた携帯電話機を用いたことにより、声紋認証のためのハードウェアを新設せずに済んでいる。

さらに、全体認証情報の入力および送信を指示するためのボタン内にＣＣＤカメラを備え、全体認証情報の入力時にボタン上に存在する指を撮像して指紋画像を得るようにしたため、使用者は１回の操作で指紋画像の入力・送信を行うことができる。このことは、特に、ボタン操作を迅速に行うことが困難な携帯電話機等の携帯端末において有利である。

また、全体認証に有効期限を設定し、有効期限内であれば全体認証を行わずとも認証代行サービスを受けられるようにしたことにより、使用者の手間を削減することができる。さらに、サイトから個別認証情報の入力を促すフォームが携帯電話機へ送信される前に、サイトにおいて個別認証情報を照合する認証プログラムに対して個別認証情報が渡されるため、使用者は当該フォームの処理をスキップして所望のページを取得することができる。

また、認証レベルを選択可能としたことにより、多種のサービスを提供可能となり、使用者が所望のサービスを受けることができる可能性が高くなっている。例えば、認証の信頼度が低下しても古い携帯電話機を継続して使用したい使用者や、信頼度が低くなっても認証処理にかかる時間を削減したい使用者や、認証処理にかかる時間や手間が増大してもセキュリティを確保したい使用者等に対して、適切なサービスを提供することができる。

さらに、複数の認証レベルを用意し、認証レベルが高い場合に保険額を低く設定したことにより、サイトにおける多様なサービスの提供と、より高い

認証レベルへの使用者の移行促進を両立することができる。また、認証代行サービス提供事業者にとっては、低い認証レベルでサービスを提供することのリスクを回避することができる。

また、本実施形態では、全体認証情報のみならず、携帯電話機の電話番号をも全体認証の必須要素としたことにより、使用者の正当性のみならず、使用者と携帯電話機との組み合わせの正当性をも認証することができる。特に携帯電話機は使用者に携帯されるものであるため、使用者の行動を制約することなく、高い精度で全体認証を行うことができる。

また、本実施形態では、サイトのシステムに変更を加えることなく、端末装置からサイトを利用する会員に、容易かつ安全に利用することができる認証サービスを提供する事を可能とし、サービスの提供価値を向上することができる。また、使用者においては、多様なサービスを容易かつ安全に利用できることになるから、認証を要する会員制サービスの利用意欲の向上を期待できる。

産業上の利用可能性

本発明は、認証情報の入力を要するサイトが提供するサービスの利用意欲を向上させることができる認証システム、ならびに当該認証システムを構成する認証代行装置および端末装置を提供する。

請 求 の 範 囲

1．通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第１のデータベースと、

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第１の手段と、

第１の手段により認証された使用者が利用を希望するサイトを特定する第２の手段と、

第１のデータベースを参照して、第１の手段により認証された前記使用者と第２の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第１の情報を渡す第３の手段とを有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

2．前記端末装置が生体に固有な情報を取得する第４の手段を有し、当該生体に固有な情報を使用して前記端末装置の使用者を認証することを特徴とする請求項１に記載の認証処理システム。

3．前記生体に固有な情報が指紋情報および声紋情報を含むことを特徴とする請求項２に記載の認証処理システム。

4．前記生体に固有な情報が指紋情報を含むことを特徴とする請求項２に記載の認証処理システム。

5．前記生体に固有な情報が声紋情報を含むことを特徴とする請求項２に記

載の認証処理システム。

６．前記端末装置に固定された情報が当該端末装置の電話番号であることを特徴とする請求項１に記載の認証処理システム。

７．通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第１のデータベースと、

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第１の手段と、

第１の手段により認証された使用者が利用を希望するサイトを特定する第２の手段と、

第１のデータベースを参照して、第１の手段により認証された前記使用者と第２の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第１の情報を渡す第３の手段と

前記第１の手段が複数の認証レベルを備え、前記使用者が当該認証レベルを選択することを可能とする第５の手段と

を有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

８．前記端末装置が当該生体に固有な情報を取得する第４の手段を有し、前記第１の手段が当該生体に固有な情報を含む情報を使用して前記端末装置の使用者を認証することを特徴とする請求項７に記載の認証処理システム。

９．前記端末装置に固定された情報が当該端末装置の電話番号であることを特徴とする請求項７に記載の認証処理システム。

１０．通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第１のデータベースと、

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第１の手段と、

第１の手段により認証された使用者が利用を希望するサイトを特定する第２の手段と、

第１のデータベースを参照して、第１の手段により認証された前記使用者と第２の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第１の情報を渡す第３の手段と、

前記第１の手段で前記使用者が認証レベルを選択することを可能とする第５の手段と、

前記第５の手段により前期認証レベルに基づいて、当該使用者に対する保険料を請求する手段を有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

１１．前記端末装置が当該生体に固有な情報を取得する第４の手段を有し、前記第１の手段が当該生体に固有な情報を含む情報を使用して前記端末装置の使用者を認証することを可能とすることを特徴とする請求項１０に記載の認証処理システム。

１２．前記端末装置に固定された情報が当該端末装置の電話番号であることを特徴とする請求項１０に記載の認証処理システム。

１３．通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

前記複数のサイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第１のデータベースと、

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第１の手段と、

第１の手段により認証された使用者が利用を希望するサイトを特定する第２の手段と、

第１のデータベースを参照して、第１の手段により認証された前記使用者と第２の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第１の情報を渡す第３の手段と、

第１の手段によって認証される認証の効果の有効期限を管理する第７の手段とを有し、前記移動網に接続した

認証代行装置と

を有する認証処理システム。

１４．前記端末装置が当該生体に固有な情報を取得する第４の手段を有し、前記第１の手段が当該生体に固有な情報を含む情報を使用して前記端末装置の使用者を認証することを可能とすることを特徴とする請求項１３に記載の認証処理システム。

１５．前記端末装置に固定された情報が当該端末装置の電話番号であることを特徴とする請求項１３に記載の認証処理システム。

１６．通信網と、

生体に固有の情報を含む情報を取得する第４の手段と、取得した生体に固有の情報を認証前段処理する第８の手段とを有し、前記通信網に通信手段を介して接続できる複数の端末装置と、

前記通信網に接続した複数のサイトと、

前記端末装置の使用者を、前記第８の処理で処理された情報を利用して認証する第９の手段と、

前記複数のサイトに対応した複数の個別認証情報を、前記使用者に対応して格納した第１のデータベースと、

前記第９の手段により認証された使用者が利用を希望するサイトを特定する第２の手段と、

前記第１のデータベースを参照して、前記第９の手段により認証された前記使用者と前記第２の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された個別認証情報を渡す第３の手段を有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

１７．通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

前記複数のサイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第１のデータベースと、

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第１の手段と、

第１の手段により認証された使用者が利用を希望するサイトを特定する第２の手段と、

第１のデータベースを参照して、第１の手段により認証された前記使用者と第２の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第１の情報を渡す第３の手段と、

前記第２のデータベースを、前記複数のサイトが更新することを可能とする第１０手段を有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

１８．複数の端末装置と通信網を介して接続できて、複数のサイトに通信網を介して接続できて、

前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第１のデータベースと、

前記個別認証情報の種類と属性を含むサイト情報を、当該サイトに対応して格納した第２のデータベースと

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第１の手段と、

第１の手段により認証された使用者が利用を希望するサイトを特定する第２の手段と、

前記第１のデータベースを参照して、前記第１の手段により認証された前記使用者と前記第２の手段により特定されたサイトとに対応した第１の情報を抽出して、当該サイトに抽出された第１の情報を渡す第３の手段とを有する

認証代行装置。

１９．複数の端末装置と通信網を介して接続できて、

複数のサイトに通信網を介して接続できて、

前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第１のデータベースと、

前記個別認証情報の種類と属性を含むサイト情報を、当該サイトに対応して格納した第２のデータベースと

前記端末装置の使用者を、当該所有者に固有の生体情報を利用して認証する第１の手段と、

第１の手段により認証された使用者が利用を希望するサイトを特定する第２の手段と、

前記第１のデータベースを参照して、前記第１の手段により認証された前記使用者と前記第２の手段により特定されたサイトとに対応した第１の情報

を抽出して、当該サイトに抽出された第１の情報を渡す第３の手段とを有する

認証代行装置。

２０．通信網に接続することができる通信手段と、

前記通信網を介してサイトおよび認証代行装置に接続することができる接続手段と、

生体に固有な情報を取得する第４の手段と、

前記取得した生体に固有な情報を認証前段処理する第８の手段とを有する端末装置。

図 1

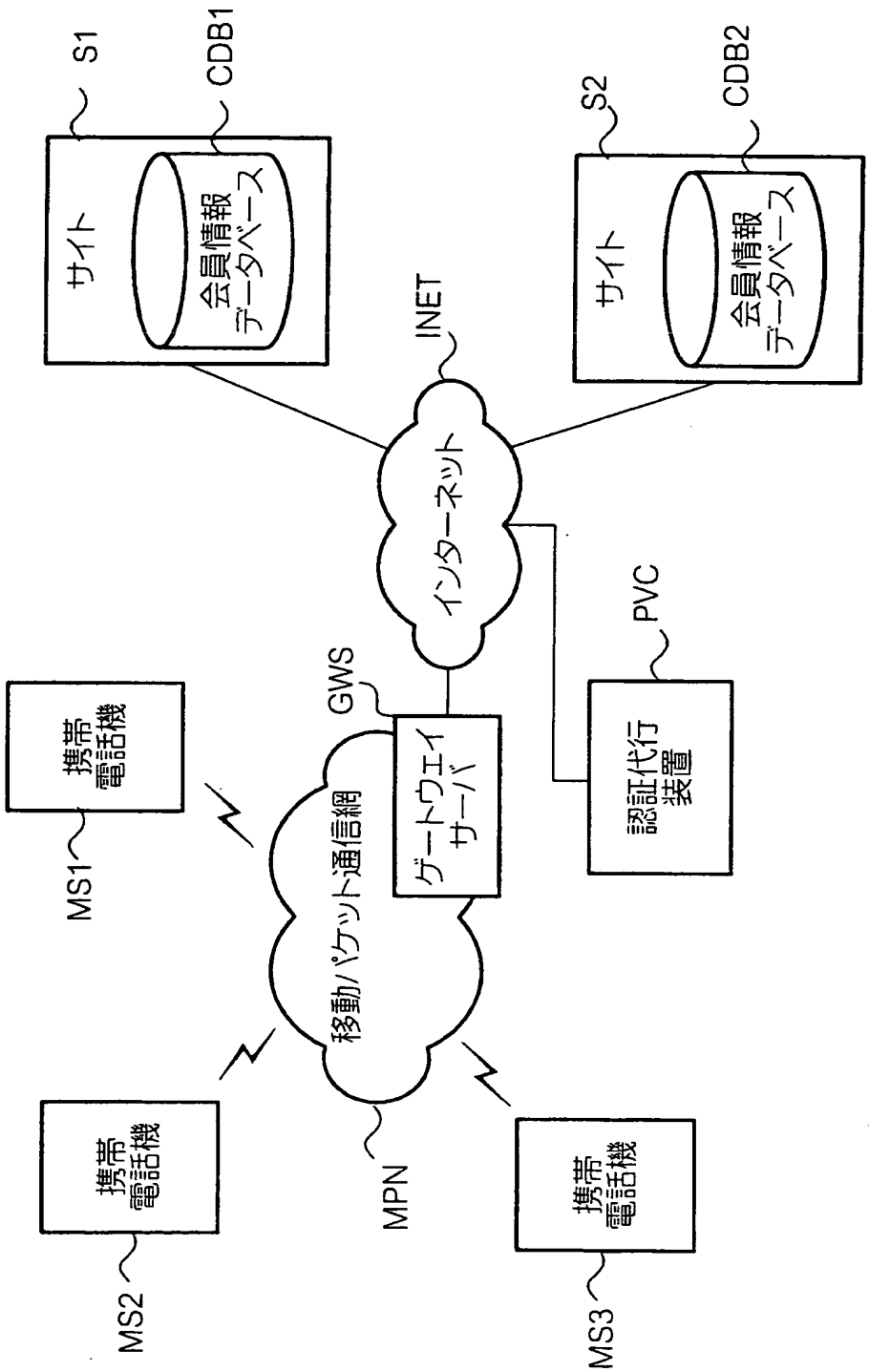

S1
CDB1
サイト
会員情報
データベース
S2
CDB2
サイト
会員情報
データベース
INET
インターネット
PVC
認証代行
装置
GWS
ゲートウェイ
サーバ
携帯
電話機
MS1
移動パケット通信網
MPN
携帯
電話機
MS2
携帯
電話機
MS3

図 2

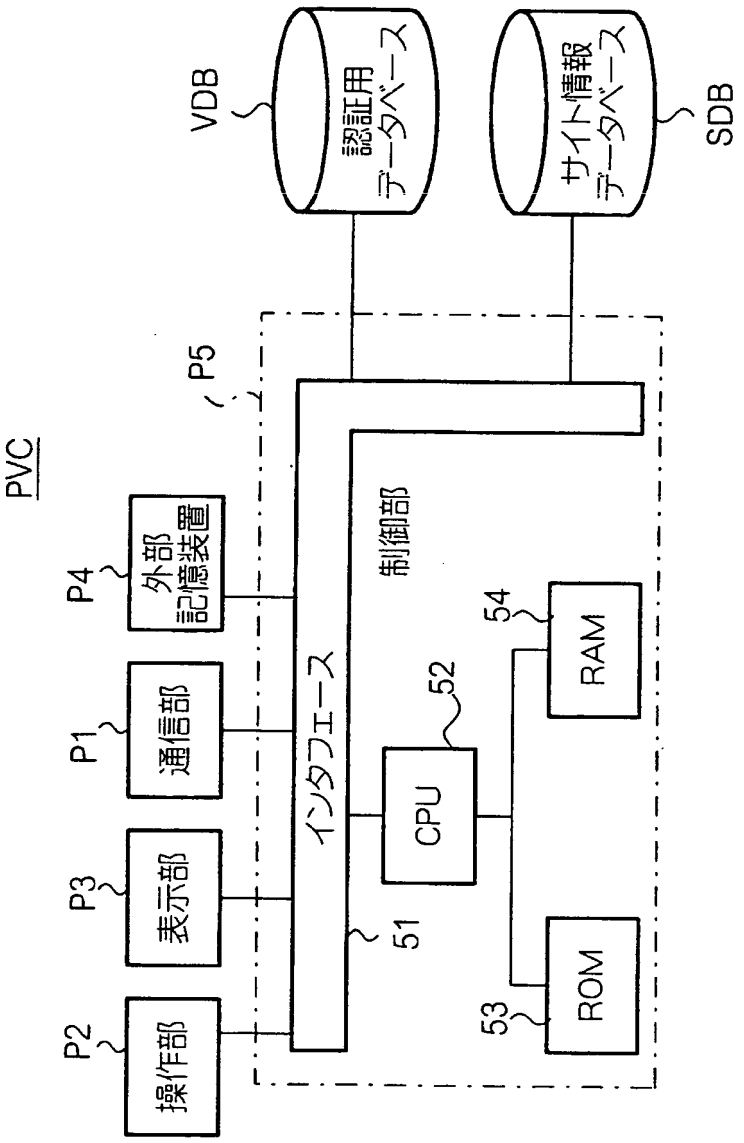

PVC
VDB
認証用データベース
SDB
サイト情報データベース
P5
制御部
P4
外部記憶装置
P1
通信部
P3
表示部
P2
操作部
インタフェース
51
CPU
52
RAM
54
ROM
53

図 3

T1

会員番号	名前	電話番号	全体認証情報			認証レベル	有効期限	接続先ID	個別認証情報		保険料	使用料
			声紋情報	指紋情報					ID	パスワード		
1	C	…	…	…		2	…	7	docom	********	0	100
								5	omocod	—		
2	B	…	…	—		1	…	5	65883	—	100	100
3	A	…	…	—		1	…	…	…	…	100	100

図 4

T2

接続先ID	タイトル	接続情報	分類	ID要否	パスワード要否	ID属性	パスワード属性
1		…	…	…	…	…	…
2		…	…	…	…	…	…
3		…	…	…	…	…	…
4		…	…	…	…	…	…
5	懸賞リスト	http://www.d.net/list/list.cgi	懸賞	要	否	4-8	…
6		…	…	…	…	…	…
7	D社ポイント	https://www.c.co.jp/point/point.cgi	ショッピング	要	要	4-8	8-16
8		…	…	…	…	…	…

図 5

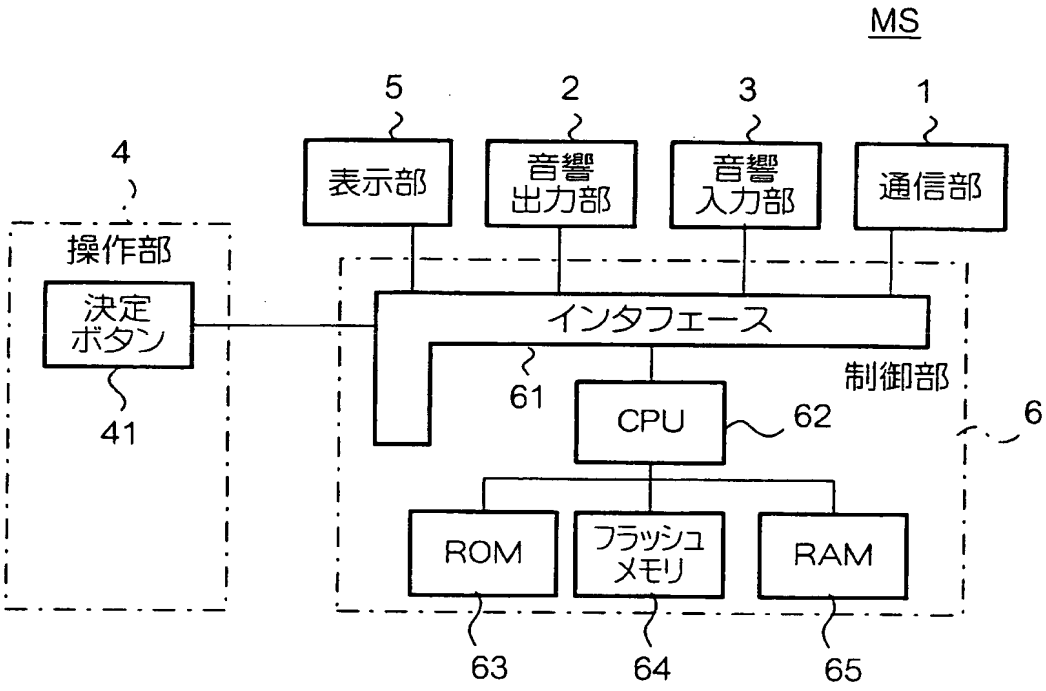

MS
5
2
3
1
4
表示部
音響
出力部
音響
入力部
通信部
操作部
決定
ボタン
インタフェース
41
61
制御部
CPU
62
6
ROM
フラッシュ
メモリ
RAM
63
64
65

図 6

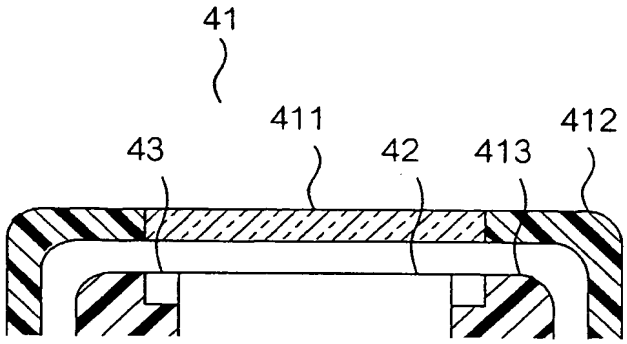

41
411
412
43
42
413

図 7

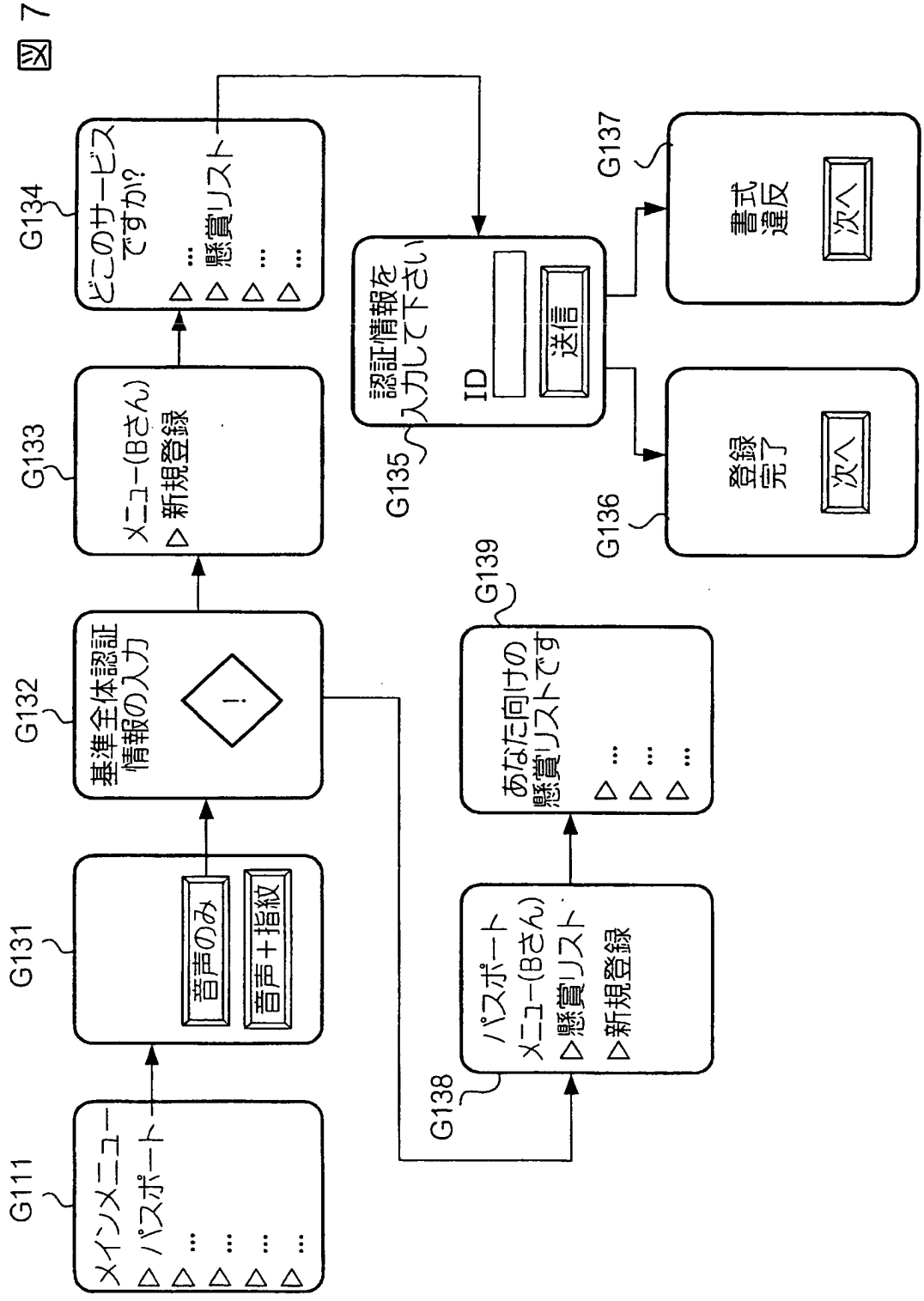

G111
メインメニュー
△パスポート
△...
△...
△...
△...
G131
音声のみ
音声＋指紋
G132
基準全体認証
情報の入力
!
G133
メニュー(Bさん)
△新規登録
G134
どこのサービス
ですか?
△...懸賞リスト
△...
△...
△...
G135
認証情報を
入力して下さい
ID
送信
G136
登録
完了
次へ
G137
書式
違反
次へ
G138
パスポート
メニュー(Bさん)
△懸賞リスト
△新規登録
G139
あなた向けの
懸賞リストです
△...
△...
△...

図 8

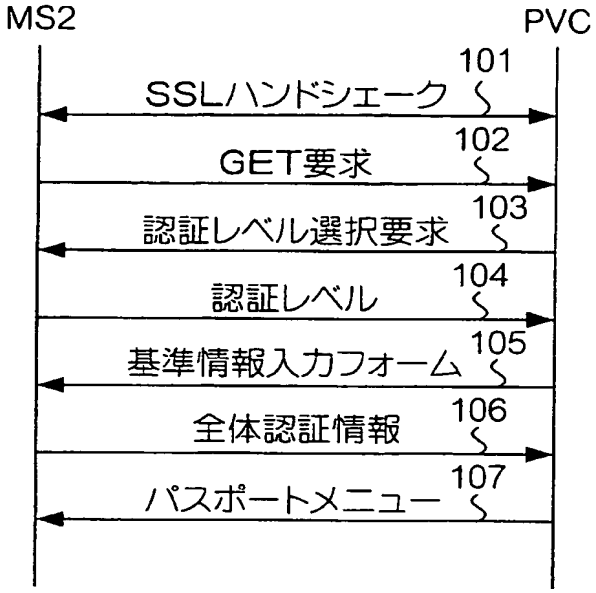

MS2
PVC
101
SSLハンドシェーク
102
GET要求
103
認証レベル選択要求
104
認証レベル
105
基準情報入力フォーム
106
全体認証情報
107
パスポートメニュー

図 9

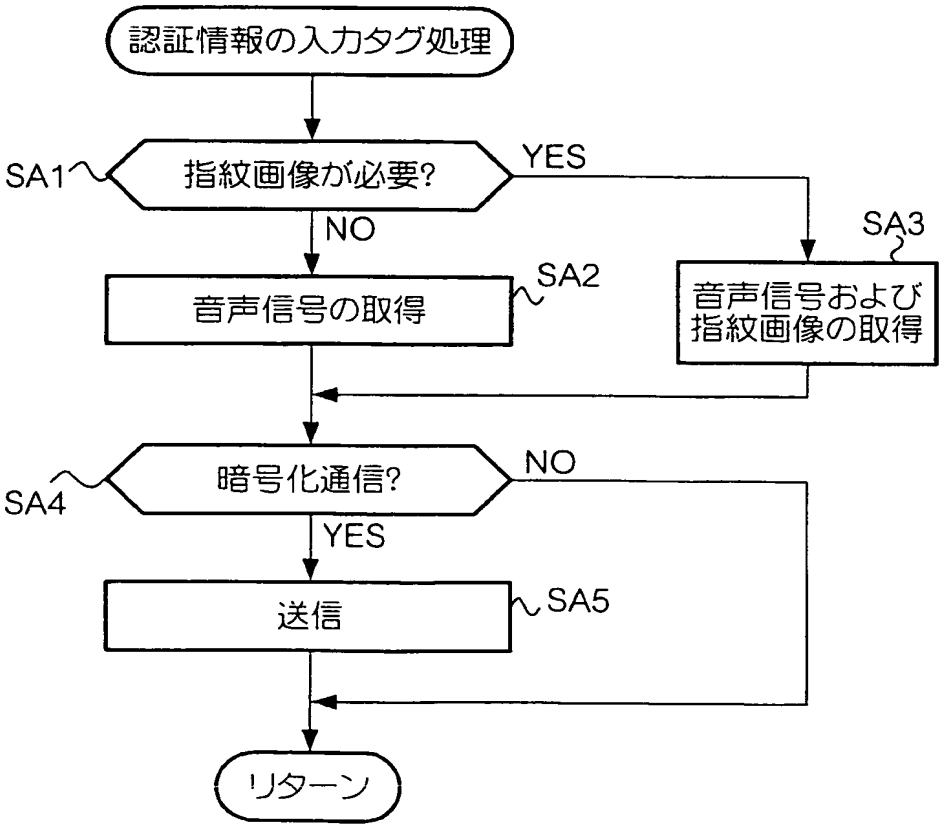

認証情報の入力タグ処理
SA1
指紋画像が必要?
YES
NO
SA3
音声信号および
指紋画像の取得
SA2
音声信号の取得
SA4
暗号化通信?
NO
YES
SA5
送信
リターン

図 10

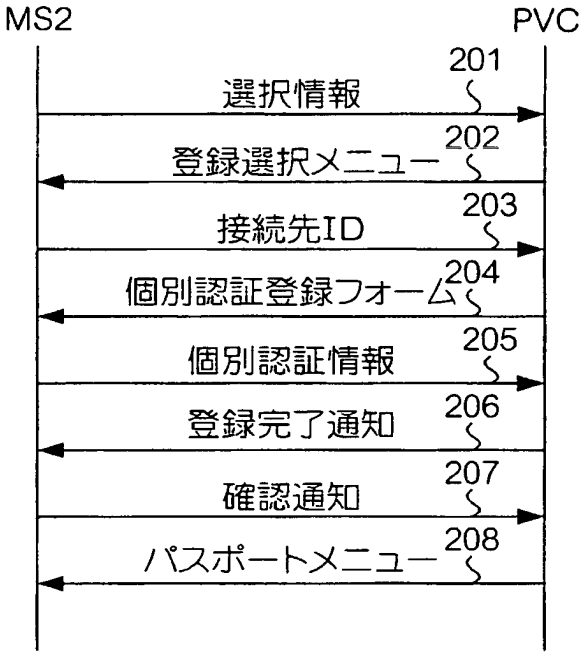

MS2
PVC
201
選択情報
202
登録選択メニュー
203
接続先ID
204
個別認証登録フォーム
205
個別認証情報
206
登録完了通知
207
確認通知
208
パスポートメニュー

図 11

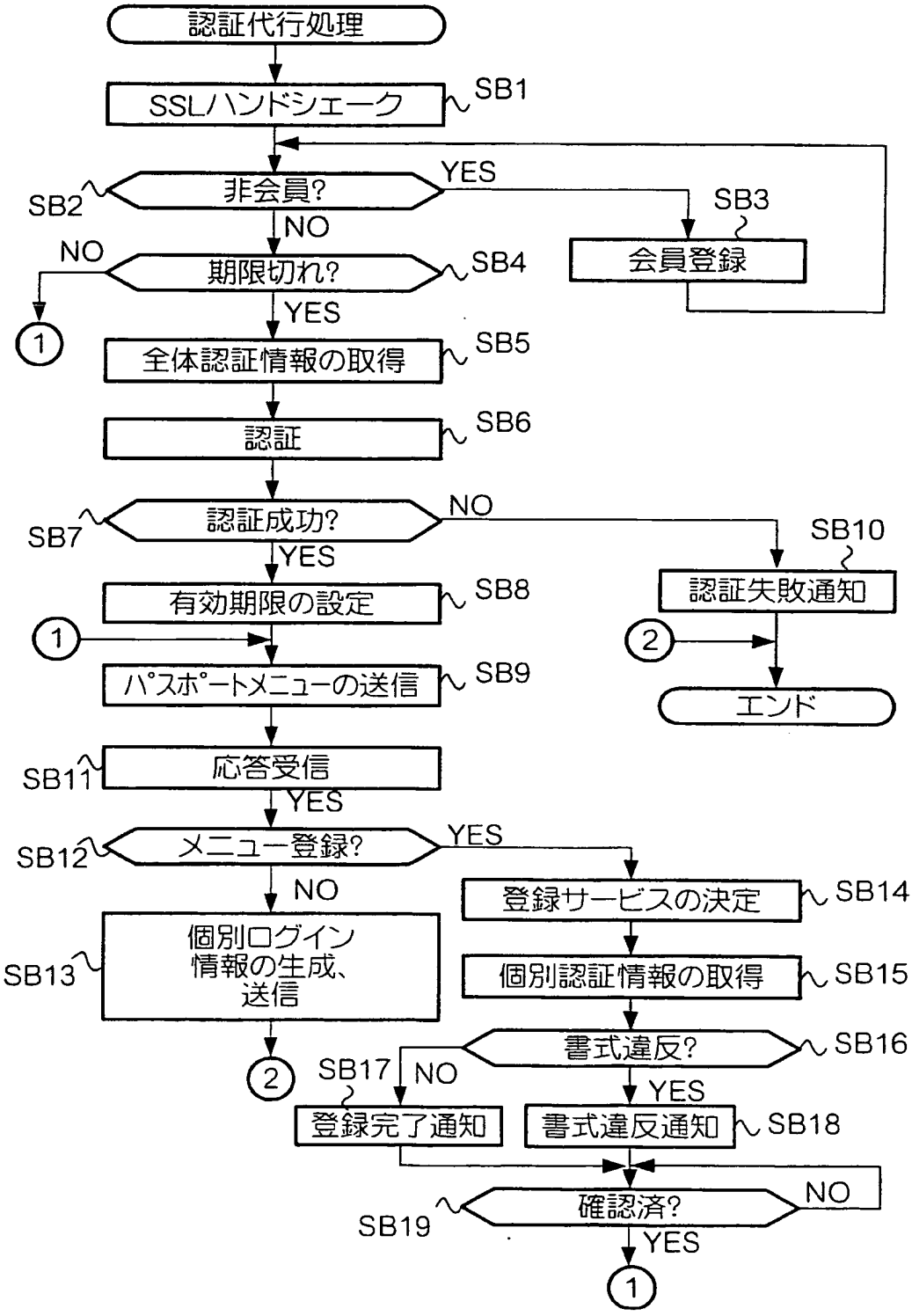

認証代行処理
SSLハンドシェーク
SB1
非会員?
YES
SB2
SB3
NO
会員登録
NO
期限切れ?
SB4
YES
1
全体認証情報の取得
SB5
認証
SB6
認証成功?
NO
SB7
SB10
YES
有効期限の設定
SB8
認証失敗通知
1
2
パスポートメニューの送信
SB9
エンド
応答受信
SB11
YES
メニュー登録?
YES
SB12
NO
登録サービスの決定
SB14
個別ログイン
情報の生成、
送信
SB13
個別認証情報の取得
SB15
書式違反?
SB16
2
SB17
NO
YES
登録完了通知
書式違反通知
SB18
確認済?
NO
SB19
YES
1

図 12

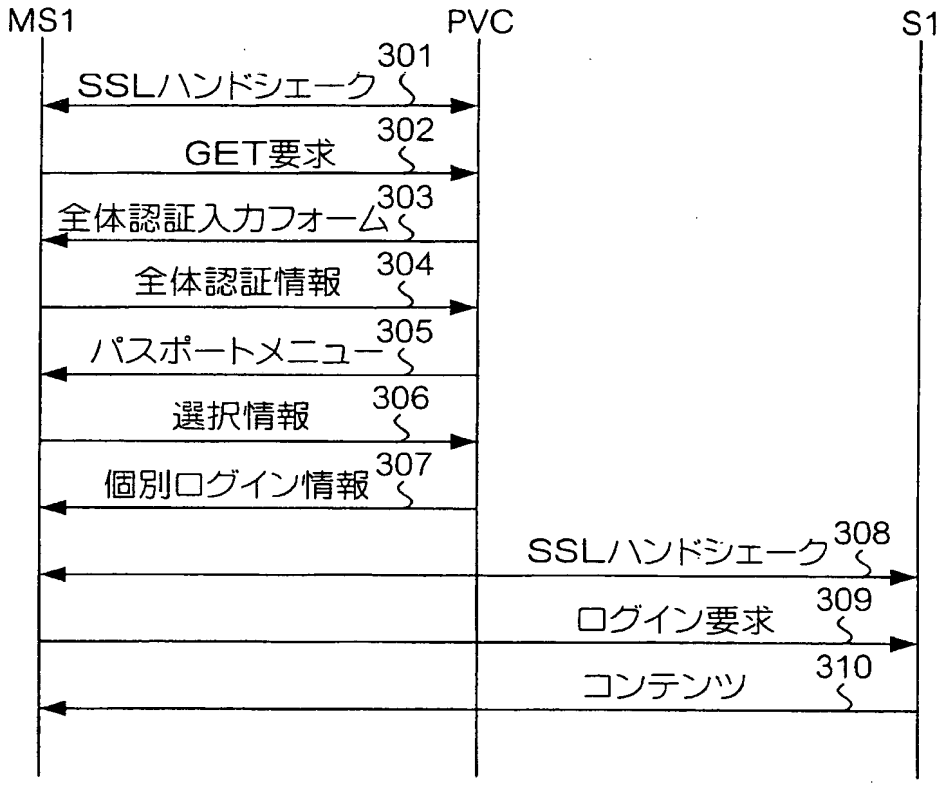

MS1
PVC
S1
301
SSLハンドシェーク
302
GET要求
303
全体認証入力フォーム
304
全体認証情報
305
パスポートメニュー
306
選択情報
307
個別ログイン情報
308
SSLハンドシェーク
309
ログイン要求
310
コンテンツ

図 13

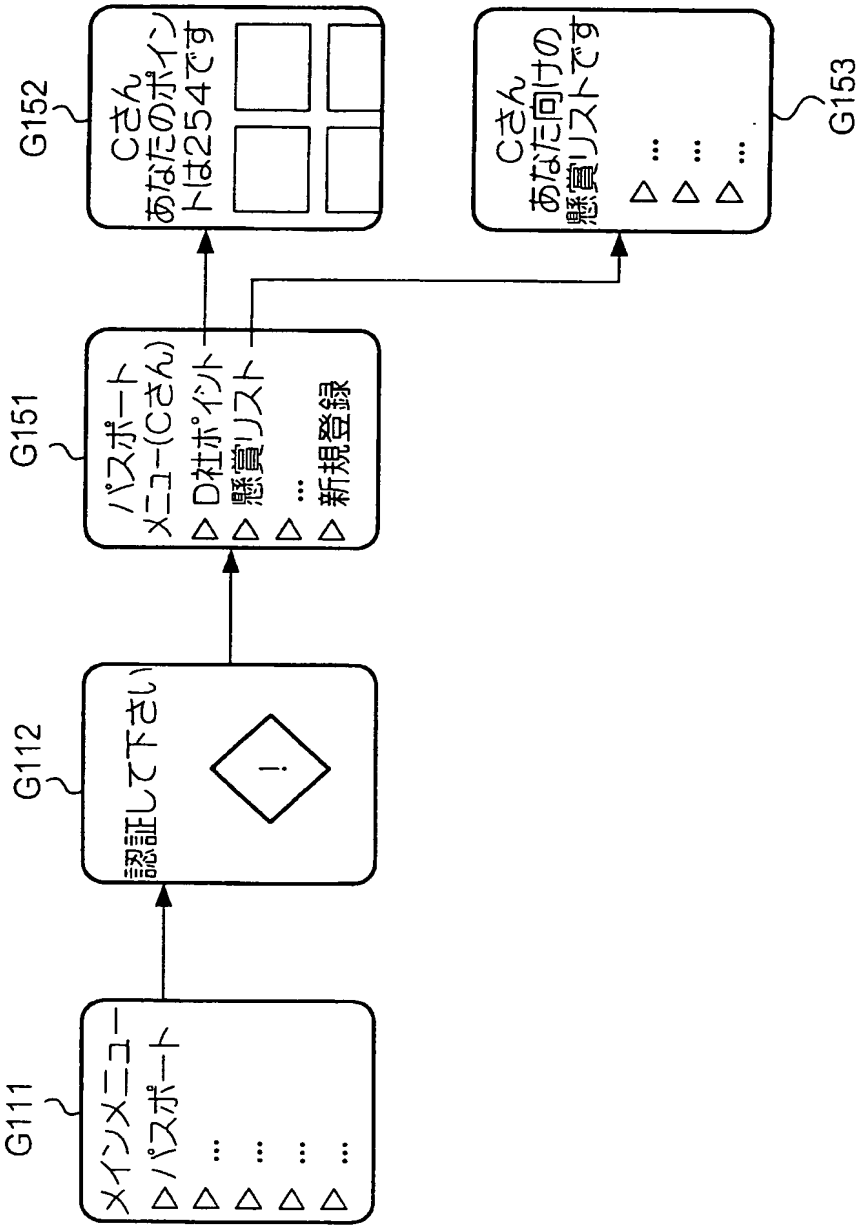

G111
メインメニュー
△パスポート
△ … … … …
G112
認証して下さい
!
G151
パスポート
メニュー(Cさん)
△ D社ポイント
△ 懸賞リスト
△ …
△ 新規登録
G152
Cさん
あなたのポイン
トは254です
G153
Cさん
あなた向けの
懸賞リストです
△ … … …

図 14

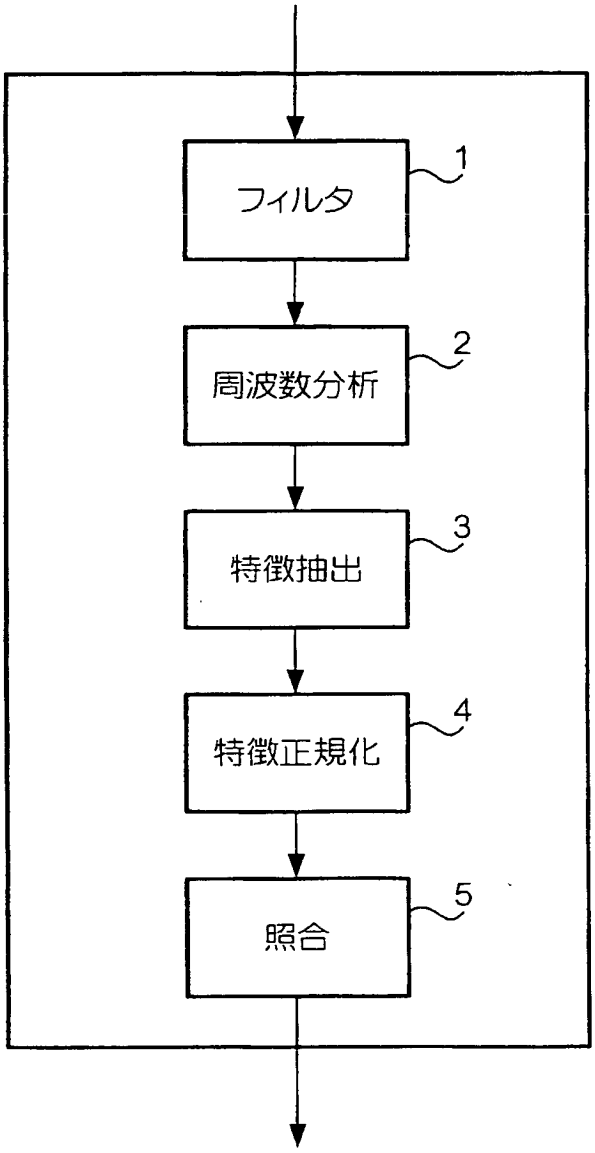


図 15

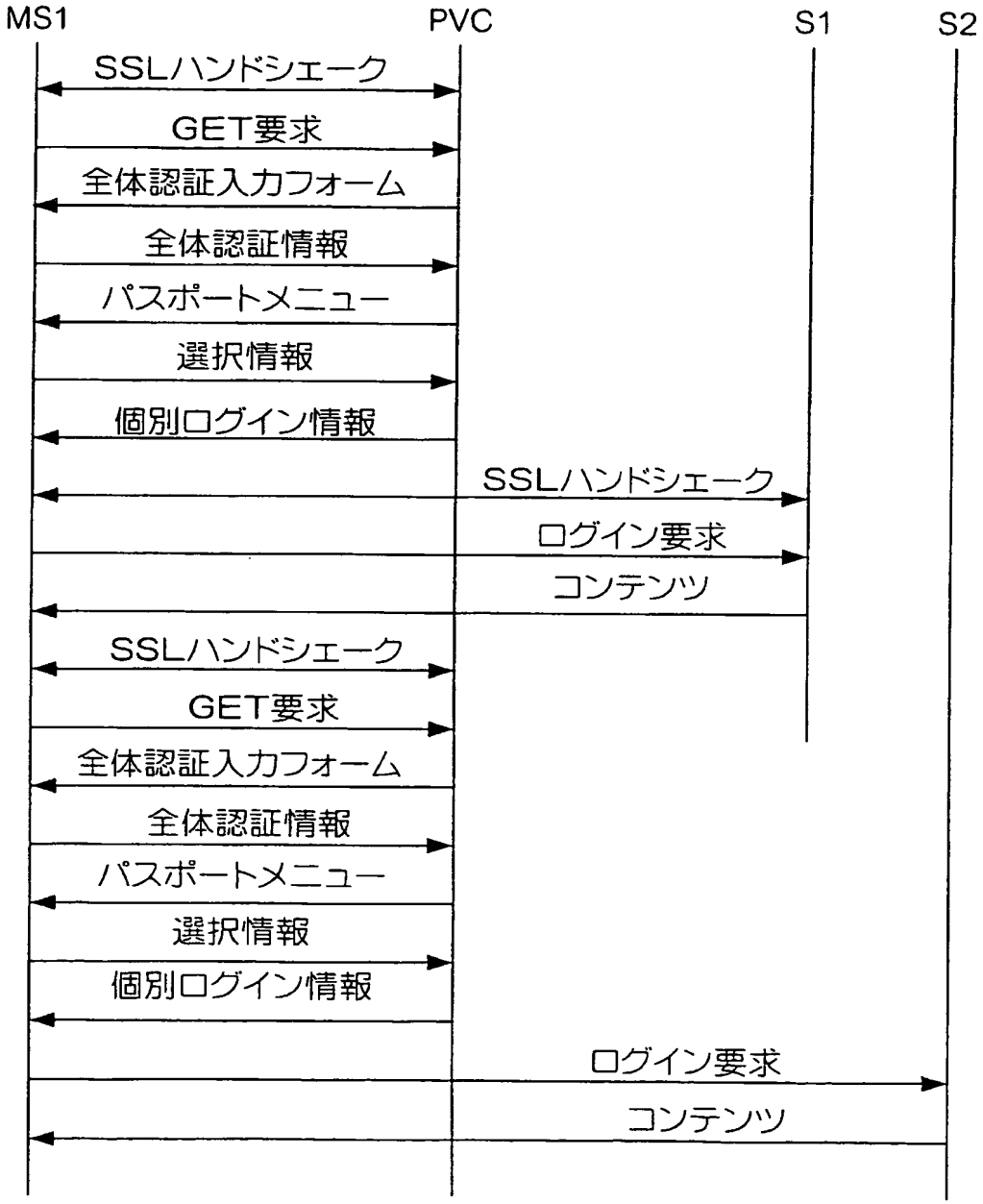

MS1
PVC
S1
S2
SSLハンドシェーク
GET要求
全体認証入力フォーム
全体認証情報
パスポートメニュー
選択情報
個別ログイン情報
SSLハンドシェーク
ログイン要求
コンテンツ
SSLハンドシェーク
GET要求
全体認証入力フォーム
全体認証情報
パスポートメニュー
選択情報
個別ログイン情報
ログイン要求
コンテンツ

図 16

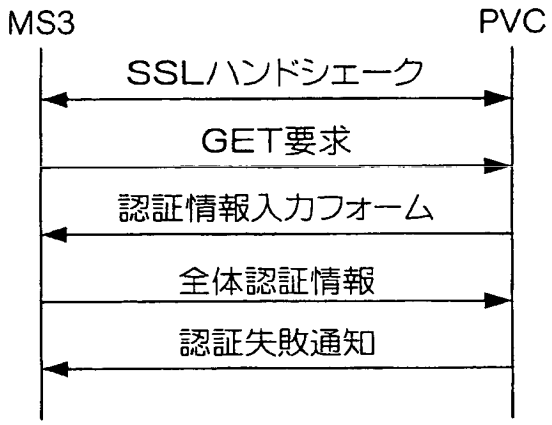

MS3
PVC
SSLハンドシェーク
GET要求
認証情報入力フォーム
全体認証情報
認証失敗通知

図 17

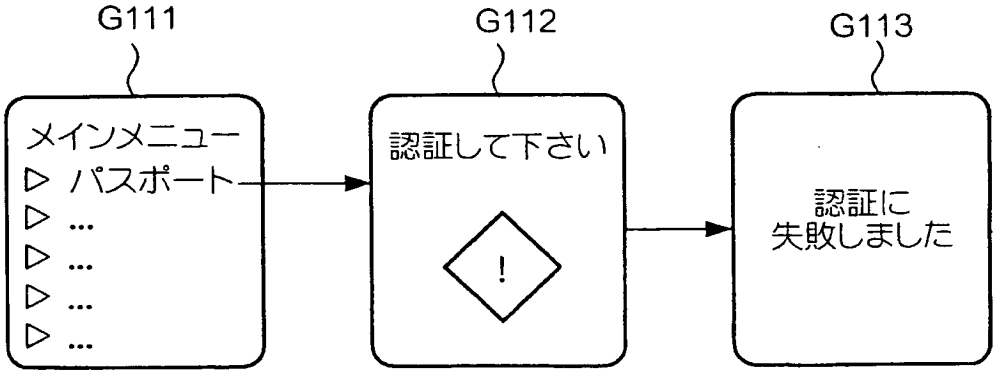

G111
G112
G113
メインメニュー
▷ パスポート
▷ ...
▷ ...
▷ ...
▷ ...
認証して下さい
!
認証に
失敗しました

図 18

認証レベル	照合情報	保険料
1	音声信号	100
2	指紋画像	50
3	指紋画像および音声信号	0

図 19